

**Surveillance
globale:
ENQUETE SUR
LES NOUVELLES**

Eric Sadin

VISIT...

LANZAROTE
Caliente.COM

ÉRIC SADIN

SURVEILLANCE
GLOBALE

ENQUÊTE SUR LES NOUVELLES
FORMES DE CONTRÔLE

CLIMATS

ÉRIC SADIN

SURVEILLANCE
GLOBALE

ENQUÊTE SUR LES NOUVELLES
FORMES DE CONTRÔLE

CLIMATS

Éric Sadin

SURVEILLANCE
GLOBALE

ENQUÊTE SUR LES NOUVELLES
FORMES DE CONTRÔLE

CLIMATS

Sadin Éric

Surveillance globale

Enquête sur les nouvelles formes de contrôle

Flammarion

Maison d'édition : Climats

© Climats, un département des éditions Flammarion, 2009

Dépôt légal : février 2009

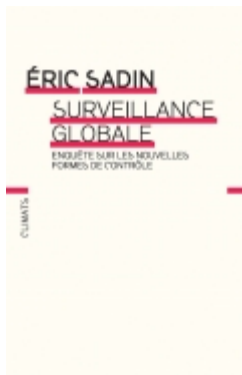
ISBN numérique : 978-2-0812-3545-8

N° d'édition numérique : N.01EHBN000108.N001

Le livre a été imprimé sous les références :

ISBN : 978-2-0812-2297-7

Ouvrage composé et converti par [Nord Compo](#)



La surveillance : plus personne n'oserait en douter. Mais quelle forme prennent les nouveaux dispositifs de contrôle et en quoi sont-ils différents des pratiques du siècle dernier ? Comment le monde et aux autres ? Vont-ils jusqu'à menacer le droit à la vie privée ? Telles sont les questions que reprend ainsi un débat ancien sous un jour totalement nouveau. Car il ne s'agit plus de surveillance ciblée pour déceler les comportements déviants et les punir, mais de prévention permanente et généralisée. Il ne s'agit plus d'observer l'espace public, mais d'accumuler des données sur chaque individu, considéré sinon comme un terroriste en cible marketing, ou un voisin à espionner. S'organise ainsi un scannage ininterrompu de la frontière entre surveillant et surveillé, entre monde physique et monde virtuel. Au lieu de nous ou alimentons à notre insu - vidéosurveillance, géolocalisation, bases de données, logiciels d'analyse comportementale un Big Brother désincarné, dont nous sommes à présent désormais en chacun de nous. Mêlant l'enquête à la réflexion, cet essai explore les multiples enjeux de la surveillance contemporaine, et incite chacun à réagir face au volontaire.

DU MÊME AUTEUR

Deux-points, Pécuchette éditions, 1999.

7², Les Impressions Nouvelles, 2002.

Nihon No kigo, Signes du Japon, Onestar Press, 2003.

Times of the signS/Bangkok, Bangkok, Art4D, 2004.

Poésie atomique, éc/artS essais, 2004.

Tokyo, P.O.L, 2005.

Times of the signS, Birkhäuser, 2007.

Globale Paranoïa, Les petits matins, coll. « Les grands soirs », 2009 (poésie).

« Le troisième millénaire commencera par une guerre diffuse et permanente. »

Maurice Schumann

« Je dois vous prévenir : tout ce que vous pensez peut être retenu contre vous. »

Philip K. Dick,
Souvenirs à vendre

« La Révolution sera complète quand le langage sera parfait. »

George Orwell, *1984*

INTRODUCTION

Un « bouillon de culture » inédit

Moment historique décisif

Notre période est caractérisée par une accélération sans précédent de l'histoire de la technique, dont les effets sont particulièrement sensibles au prisme de quatre événements majeurs : 1/ *extension ininterrompue du numérique* ; 2/ *développement des réseaux de télécommunication* ; 3/ *essor des nanotechnologies* ; 4/ *recherches liées aux biotechnologies et aux manipulations génétiques*. La plupart des innovations actuelles s'efforcent d'exploiter ce que chacune de ces dimensions autorise séparément, mais plus encore les effets d'*interconnexion* entre les deux premières (par exemple Internet représente le protocole le plus emblématique issu de l'entrecroisement entre numérique et télécommunication) ; parfois l'association entre trois d'entre elles (le séquençage du génome articule : calcul algorithmique / échange d'informations ou délégation de tâches via des réseaux entre centres de recherche / application biologique) ; de surcroît, l'introduction appelée à se généraliser de puces électroniques dans le corps, reliées à des bases de données, annonce l'entrelacement indissociable de ces quatre champs, aux incidences anthropologiques considérables. Le développement plus ou moins enchevêtré de ces quatre secteurs déterminera la quasi-totalité des usages professionnels, domestiques, culturels à venir, selon une cartographie où des technologies en expansion incessante interagiront sans cesse davantage, dessinant quelques-unes des *mailles* décisives qui structureront le XXI^e siècle.

L'extrême vitesse avec laquelle ces bouleversements se déploient et « pénètrent » notre environnement constitue une caractéristique inédite. Conception et production ininterrompues de procédés et protocoles sans cesse renouvelés, aussitôt suivis de leur prompt obsolescence, s'enchaînent à des cadences croissantes et exponentielles¹. La *pression technologique* impose d'autres structures temporelles qui correspondent au passage du régime de la *successivité* à celui de la *prolifération* ininterrompue d'événements, qui font circuler flux d'*éclosions* et d'*entropies* selon une quasi-simultanéité ; figures en mutation constante qui interdisent des modalités de perception stables, et

ébranlent quantité de classifications et de repères historiques. Désormais, la dimension de *transformation* que suppose la temporalité constitue un phénomène partout sensible – parfois jusqu’au vertige – dans notre environnement contemporain (usage quotidien et massif de procédés ou d’objets très récents, « versions » de produits continuellement modifiées, capacités de stockage et puissances de calcul régulièrement démultipliées...). Il se développerait depuis peu une sorte de conscience (encore trop insuffisamment partagée) lucide du « mouvement perpétuel » qui imprime le cours des choses. Cette perception de l’« impermanence » du monde (pensée zen), à l’œuvre depuis des siècles en Asie, permet à cette partie du globe de s’inscrire activement dans un *milieu* désormais marqué par une *instabilité* continue.

L’ampleur et la densité de ces mutations – alors qu’elles *ouvrent* de nouveaux champs d’exploration et d’invention – suscitent peur et anxiété, tétanisent esprit d’initiative et propension au risque, au profit d’une aspiration instinctive à *maintenir* des situations, à se « protéger » de dangers entendus comme venant presque toujours de l’« extérieur ». Il est probable que l’extension des technologies de surveillance dans notre environnement représente – parmi bien d’autres raisons que nous analyserons au cours de notre enquête – une sorte d’inconscient collectif effrayé par la puissance de soubresauts soudains et inédits, qui chercherait à renforcer la tentation du *contrôle*. Les effets de dilution des pouvoirs centraux, de fragmentation des instances de décision, de l’éparpillement des risques, demeurent communément associés à une globalisation perçue comme déstabilisante et angoissante, tramée de lois immaîtrisables, autant que par une extrême et récente *atomisation* expansive des rapports de force.

La chute du mur de Berlin en 1989 inaugure la fin d’une organisation bipolaire qui régissait les relations entre nations, et qui plus largement encore imprégnait de nombreux schémas conceptuels, politiques, économiques, fondés sur des logiques d’opposition binaire. La dernière décennie du XX^e siècle témoigne d’une *diffraction* de points de pouvoir compacts vers une *expansion* du nombre de territoires désormais autonomes (éclatement de l’Union soviétique, de la Yougoslavie, de la Tchécoslovaquie). Ces événements signalent un phénomène généralisé, repérable selon des logiques fractales, à l’intérieur d’autres échelles (par exemple la loi de décentralisation en France de 1982-1983, conférant de nouvelles compétences aux collectivités locales, ou la mise en place progressive d’un réseau de régions européennes...). L’événement du 11 septembre 2001, l’agression de la première puissance économique et militaire par un groupuscule d’individus *disséminés*, confirme à l’excès une des nouvelles données décisives de notre contemporanéité : celle de l’extrême *fragmentation* des rapports de force entre entités politiques ou idéologiques, rendant impossibles les principes réguliers d’affrontements entre forces identifiées et circonscrites, par le fait de

l'éclatement de certaines d'entre elles, de leur localisation incertaine et dispersée, de leur *mobilité* continue.

Le début du XXI^e siècle est marqué par le phénomène de l'*atomisation*, qui découvre une amplification incessante de *nœuds* de décision et d'expression (foyers de pouvoirs variés, presse, associations, ONG, syndicats, regroupements occasionnels, forums d'échanges...) ². D'une certaine façon, la généralisation du réseau Internet est à la fois emblématique de ces jeux d'éclatement et les intensifie à la faveur de l'architecture technique qui autorise une quasi-infinité de sources de réception et d'émission singulières : les adresses IP. En outre, la propagation exponentielle du nombre de sites et de pages Web contribue au foisonnement croissant des volumes informationnels, que les moteurs de recherche s'efforcent d'identifier et dont les régulières mises à jour effectuées par les robots fureteurs signalent les effets de « débordement » continu, comme autant de signes de l'impossibilité de fixer les flux contemporains. L'ampleur et la *dispersion* des risques de toute nature se sont considérablement accrues et constituent désormais une donnée structurante de notre environnement. Le spectre des menaces contribue à l'installation – parfois légitime, parfois hystérique – de dispositifs et à l'accélération de la conception de nouveaux protocoles, à la prise de décisions politiques et légales souvent hâtives ³.

Les formes actuelles et en devenir de la surveillance se situent au cœur de nombreuses problématiques et interrogations contemporaines ; une méthodologie exigeante appelle à repérer les multiples *ramifications* qui les structurent, à ne pas réduire le large ensemble qu'elles forment, à saisir leur caractère *composite* et les différentes applications qu'elles autorisent. Ce sont notamment la nature de leur extension, leur structuration technique, leur efficacité et leur précision, les cadres légaux qu'elles perturbent, le droit à la vie privée qu'elles peuvent menacer, qui constituent autant de questions que nous examinerons au cours de cet ouvrage. Il s'opère, d'une certaine façon, une condensation d'enjeux et d'incidences extrêmement hétérogènes, d'ordre technique, politique, économique, juridique, éthique, culturel, qui s'entrelacent et obligent à la mise en place d'une enquête nécessairement *pluristratifiée*, contrainte par la force de la mutation ininterrompue des événements, de tenir l'ensemble de ces lignes comme l'analyse d'une situation provisoire, probablement soumise à des principes d'intensification continus.

La surveillance : une notion multifonctionnelle

Les caractéristiques de la surveillance que nous allons étudier dans leurs formes contemporaines ne renvoient pas à une vague entité unifiée, mais se définissent par des *objectifs* qui varient selon les visées et la nature des « cibles ». Une des fonctions majeures consiste à tenter d'identifier la menace

avant qu'elle ne se produise : être en mesure de se préparer en conséquence et de la contrer. Elle relève d'une *dimension informationnelle* : la collecte des justes indices qui avertiraient des dangers avant qu'ils ne puissent advenir. (Par exemple, la déroute américaine de Pearl Harbor en décembre 1941 est due à une défaillance du système de surveillance, qui n'a pas su *décrypter* la mise en place d'une attaque *surprise*, qui représente l'impératif absolu à éviter : ne pas être pris au dépourvu face à l'ennemi.) Ce souci qui s'applique à percer la nature des risques potentiels appartient à une longue histoire, celle de la nécessité pour les nations et les instances de pouvoir de protéger les territoires et de maintenir une assise politique stable ; l'enjeu étant de *devancer* les dangers exogènes (infiltrations, tentatives de déstabilisation, guerres...), autant qu'endogènes (révoltes, complots, coups d'État...).

Cette quête de *données* constitue une dimension actuelle majeure, particulièrement à l'œuvre dans ce qui est qualifié de « menace terroriste », pour laquelle s'est opéré un glissement décisif – mais non exclusif – vers le privilège accordé au *renseignement* (*Intelligence*), au détriment des armes d'affrontement direct habituellement requises dans le cadre de guerres dites « conventionnelles ». La « traque de signes » représente depuis l'effondrement de l'empire soviétique la première priorité des stratégies de défense, et ce, simultanément à un essor sans précédent de la « société de l'information ». La surveillance correspond d'abord à une collecte d'indices menée *en amont*, qui se déploie désormais dans un contexte marqué par la production de quantités d'objets de captation et de diffusion de flux textuels, iconiques et sonores, qui à la fois amplifient les volumes, perturbent l'ambition d'une interception stabilisée, et sont soumis à des puissances d'analyse et de traitement sans cesse augmentées et sophistiquées.

Les technologies de surveillance sont encore destinées à *avertir* le plus rapidement d'une menace en cours, à *détecter* et à *signaler* par des dispositifs adéquats la présence d'un danger plus ou moins imminent (les radars aériens répondent exactement à cette fonction ; les barbelés électroniques ; les sonneries d'alarme en cas de violation d'un périmètre protégé ou d'un véhicule...). Depuis l'extension du numérique, la faculté d'alerte autorisée par l'*interconnexion* généralisée s'est considérablement accrue, selon des délais quasi instantanés, nommés « temps réel » (terme en partie erroné car du différé – même infime – persiste malgré tout). L'enjeu technique ne consiste plus désormais à le réduire mais à garantir pertinence et fiabilité des systèmes. Pour ceux qui sont supposés être les « cibles », il ne s'agit pas d'allonger le répit qui serait dérisoire mais de disséminer de fausses pistes, de propager des leurre : stratégies de ripostes les plus efficaces à l'encontre de la puissance du signal en « temps réel ». Nous reviendrons largement sur la fonction d'*alarme* qui constitue dorénavant une des modalités prioritaires de la surveillance, permise par l'amplification du nombre de bases de données associées à des logiciels de reconnaissance capables d'*identifier* des individus ou des objets et

d'en aviser le cas échéant des centres de contrôle gérés par des personnes et/ou des systèmes électroniques.

Quantité de procédés ont été développés depuis des siècles en vue de répertorier les individus, de renvoyer les corps à des identités fixées et classifiées. Tous supposent l'inscription de coordonnées sur des supports qui se sont modifiés au cours des âges. L'usage du papier s'est imposé depuis la Renaissance jusqu'à nos jours. Ce qui caractérise notre temps présent est une *double* utilisation de documents imprimés qui renvoient désormais à des fichiers numériques. Une carte d'identité, de Sécurité sociale, un passeport (pièces en papier ou en plastique) contiennent des informations capables d'être lues grâce à des puces ou des bandes magnétiques. Mais ce qui caractérise encore notre temps présent est l'amplification de la *biométrie* qui réduit le corps à des codes chiffrés et indexés, inscrivant le souci ancestral de l'identification dans un tout nouveau type de rapport : celui d'une analyse en temps réel de certaines propriétés biophysiques (empreintes, main, rétine, iris, visage, reconnaissance vocale...). L'association entre techniques biométriques et introduction de puces dans les organes rendra obsolète le port de documents d'identité ou de cartes de toutes sortes, au profit d'un *repérage* immédiat des personnes par l'intégration dans l'environnement de capteurs connectés à des bases de données, situant désormais chaque être comme une surface susceptible d'être « scannée » et de s'exposer comme un plan recouvert d'informations – relatives à quantité de ses activités et à sa *vie privée*.

Pouvoir distinguer des personnes suspectes ou condamnées – en étant vu ou non, selon les cas – constitue un moyen ancestral de vérifier la conduite des individus, d'anticiper les risques grâce à la « transparence de la perspective » mise en place. Cette ambition est indissociable de l'élaboration de *systèmes techniques* (miradors, meurtrières, œils-de-bœuf, jumelles, survol aérien, agencements architecturaux – citons, par exemple, un des plus sophistiqués d'entre eux : le fameux *Panopticon* de Jeremy Bentham). Depuis une trentaine d'années, l'apparition de la *vidéosurveillance* a offert une puissance démultipliée de vision, devenue ubiquitaire. En outre, les caméras thermiques à vision nocturne ont rendu possible une continuité dans le temps. L'observation des corps est désormais médiatisée par quantité d'écrans qui exposent des êtres sous forme de pixels. Plus encore, la récente connexion des circuits vidéo à des logiciels de reconnaissance (« vidéosurveillance intelligente »), d'une part délègue le « regard » au calcul électronique, et d'autre part inscrit chacun comme devant faire l'objet d'une analyse de comportement et des traits du visage, réduits à des codes transmis à des bases de données, capables de *signaler* tout suspect. L'individu du XXI^e siècle se trouve continuellement soumis à des procédures d'« indexation » évolutives, en fonction des *traces* numériques qu'il *dissémine* au cours de ses déambulations physiques ou de ses navigations virtuelles.

Chaque action préméditée entre personnes ou entités distinctes suppose un

acte de communication. L'*interception* d'informations offre la solution la plus efficace pour prendre connaissance de la préparation d'une opération. Ce souci a historiquement favorisé la pratique de l'espionnage, dont l'activité consiste prioritairement à recueillir des renseignements et à les analyser. Les modalités de transmission se sont progressivement modifiées (lettres, télégrammes, conversations téléphoniques, fax, emails...). Un moyen privilégié de contrer les intrusions consiste à brouiller les échanges afin de les rendre seulement lisibles à ceux connaissant les « clés », à pratiquer l'*encryptage*. Le développement du numérique a considérablement généralisé son usage (ainsi que celui de son pendant : le *décryptage*) ; les deux technologies représentent aujourd'hui un champ de recherche et une activité considérable de la surveillance contemporaine, confrontée à la circulation expansive et ininterrompue de messages, dont une large masse nécessite une confidentialité absolue (données bancaires, par exemple), alors que d'autres doivent être surprises et justement *interprétées* en vue de témoigner d'éventuelles menaces en cours.

Une ambition historique de la surveillance consiste à *localiser* corps ou objets dans l'espace, soit en vue de suivre des individus déjà repérés, soit, après des délits commis, en vue de vérifier *a posteriori* un alibi ou la présence de suspects sur certains lieux. Cette visée est aujourd'hui considérablement facilitée par deux phénomènes majeurs. 1/ Les téléphones portables constituent désormais des « marqueurs spatio-temporels » qui signalent abscisses et heures exactes, grâce aux informations reçues par les antennes GSM, transmises sur les serveurs des opérateurs téléphoniques. 2/ Le système GPS (*Global Positioning System*), ou celui à venir de Galileo, crée de toutes nouvelles conditions de *cartographie* des personnes et des choses sur une surface de visibilité devenue globale, car entièrement quadrillée par la couverture satellitaire universelle. Les informations recueillies par les multiples protocoles de suivi sont *archivées* (suivant des durées qui varient selon les lois en vigueur dans chaque pays) et peuvent représenter soit des *indices* en vue d'une enquête, soit des *éléments de preuve* – après coup.

La distinction entre les fonctions *a priori* et *a posteriori* permet de discerner les différents types d'opérations susceptibles d'être effectués. La valeur d'exploitation de données stockées à la suite d'une infraction est souvent occultée par le sens commun car elle répond à une efficacité qu'on voudrait souvent ne pas voir, au profit d'un sentiment de menace diffus que représenterait la « surveillance » (on voit bien ici à quel point elle peut désigner une réalité bien vague). Nul ne s'étonne qu'après une exaction interdite par la loi, dans un État de droit, une enquête soit mise en place ; on constate que les méthodes d'investigation se sont considérablement améliorées depuis l'avènement du numérique et la généralisation des tests ADN. (Par exemple, l'identification des auteurs des attentats commis à Londres en juillet 2005 a pu être réalisée grâce au visionnage de milliers

d'heures d'images enregistrées par les caméras de vidéosurveillance de la ville.) La notion de surveillance ne renvoie pas à une finalité unique mais découvre un tissage de techniques, d'usages et de buts extrêmement *hétérogènes*, utiles pour certains, ou fortement nuisibles à l'égard des libertés publiques, pour d'autres.

Une des autres fonctions des technologies d'observation vise à décourager toute velléité « malveillante », par la mise en place de dispositifs qui revêtent également une *valeur dissuasive* (par exemple, la présence de caméras de vidéosurveillance dans les espaces urbains est souvent légitimée au nom d'un supposé pouvoir dissuasif – cependant rarement convaincant dans les faits –, nous y reviendrons). Argument qui encourage l'essor de « points de vérification », comme s'ils pouvaient ériger une sorte de « barrière virtuelle » apte à marquer la conscience collective. L'édification de protections physiques ou immatérielles (*gated communities*, polices privées, sociétés de sécurité, prolifération de codes d'accès...) impose une multitude de remparts qui recouvrent une dimension psychologique toujours plus *intériorisée*. La perception fantasmatique – caractéristique de notre temps – que suscite généralement la surveillance est indissociable du sentiment de *virtualité* qui lui est attaché : elle peut désormais être *partout*, visible – ou *invisible*.

Une de ses formes devenue majeure consiste à déployer des *techniques* en vue de stimuler la vente, en ayant recours à des savoir-faire éprouvés, sans cesse affinés : suivre les parcours effectués par les individus dans les espaces commerciaux ; analyser les pratiques d'achat de *chaque* consommateur ; dresser des profils *individualisés* et évolutifs ; fidéliser les clients devenus « membres » et leur proposer des offres « adaptées »... La mise en place de bases de données relatives aux comportements représente l'activité centrale du marketing du début du XXI^e siècle. Elle suppose de recueillir quantité de renseignements, de les traiter, de produire des statistiques, d'en déduire des constantes et de projeter des stratégies agressives et efficaces, perçues comme toujours provisoires – soumises à la modification continue des conduites et des *préférences*. Le marketing est un art de l'éveil, jamais en repos, il doit *traquer* au plus près chaque personne au sein d'une multitude composée de millions de « terminaux », tous considérés comme absolument *uniques*. Le « *tracking* » généralisé représente une des ramifications de la surveillance contemporaine la plus sophistiquée, la plus expansive, la plus sournoise, et celle jugée finalement la plus inoffensive, alors que c'est au cœur de l'utilisation de ces précieuses informations que se jouent et se joueront les questions décisives des frontières reconnues ou non du *droit à la vie privée*.

Les technologies de surveillance ne sont pas utilisées seulement par les autorités, centres de pouvoir, ou par ceux supposés se soucier de l'application de la loi (nous verrons qu'il s'opère en outre une extension inédite de formes d'observation entre individus, à structure *horizontale*), mais également par

ceux qui souhaitent commettre des délits, sous diverses modalités : connexions illégales à des circuits de caméras, violation de fichiers sécurisés, interception de codes sur les réseaux, récolte d'informations stratégiques, perturbation de protocoles électroniques... Il peut apparaître des situations *spéculaires* dans lesquelles « surveillants » et « surveillés » s'épient les uns les autres, suivant des figures fortement entremêlées – qui poussent à une *paranoïa* croissante. Nous reviendrons sur ces jeux d'intrication qui défont quantité d'idées reçues relatives au couple simplificateur dominants/dominés, au profit de figures *cristallines* qui dessinent des identités mouvantes, capables de changer de statut à tout moment et qui défient schémas et classifications figés.

L'histoire de la surveillance remonte à des temps très lointains, elle apparaît indissociable des rapports de force qui peuvent s'établir entre nations, pouvoirs, individus. Il ne s'agit pas ici de retracer une longue et complexe généalogie, mais de souligner qu'elle a toujours été liée à des *techniques* : prise de notes, instruments de vision à distance, procédés architecturaux, pièges et mécanismes d'alerte, captures photographiques, écoutes téléphoniques, enregistrements sonores... En revanche, ce qui aujourd'hui relève d'un phénomène absolument singulier renvoie à la *prolifération* de technologies qui favorisent quantités de nouvelles *applications*, renforcent leur efficacité et rapidité, facilitent la mise en place de dispositifs de contrôle *automatisés*, et autorisent une sorte de « maillage » continu des corps et des objets. La spécificité de cette situation doit encore être mise en rapport avec l'apparition de risques géopolitiques d'un autre type, qui imposent la *priorité* du *renseignement*, de l'*anticipation*, de l'*identification* de forces fragmentées. Autrement dit, la *conjonction historique* de nombreux facteurs (dont certains sont sans rapport avec les autres) contribue à une expansion ininterrompue de machines d'observation qui règle un nouveau « panoptisme » : celui du XXI^e siècle – d'une étendue et d'une puissance de « pénétration » historiquement inédites –, qui défait peu à peu et dangereusement certaines assises légales et éthiques qui ont fondé et assuré la pérennité des démocraties modernes issues des Lumières.

Conjonction de facteurs hétérogènes

L'entrecroisement récent de causes multiples produit une sorte de « bouillon de culture » composé d'« ingrédients idéaux », favorables à la formation d'un *continuum* ininterrompu de dispositifs de surveillance. Ces éléments peuvent être identifiés : généralisation de l'*interconnexion*, de la *géolocalisation*, de la *vidéosurveillance* ; constitution de *bases de données* ; développement de la *biométrie*, de logiciels d'*analyses comportementales* ; *miniaturisation* des dispositifs ; présence de plus en plus fréquente de *capteurs* et d'*étiquettes radio* (RFID) ; *menace terroriste* ; *agressivité marketing*. C'est l'ensemble de ces *couches* que nous examinerons au cours

de notre étude, chacune envisagée dans ses spécificités autant que dans leurs complexes interactions. L'inquiétude que suscite notre moment historique appelle l'élaboration d'analyses développées à l'écart d'*a priori* idéologiques réducteurs et fondées sur une conscience lucide de la dimension souvent inédite des cas de figure. L'exigence suppose de concevoir hypothèses et perspectives singulières : « Le mouvement scientifique s'est accentué violemment depuis 1900 et toutes découvertes faites depuis changent le monde, détraquant nos idées, bouleversant les notions de temps, de matière et d'espace que nous avons de toute antiquité⁴. » La puissance des bouleversements contemporains pousse à se défaire de réflexes épuisés et à instaurer des méthodologies aux modes d'approche superposés : il convient de privilégier l'*observation* au détriment de la formulation de conclusions hâtives, d'être informé des développements continus qui modifient les situations, de pénétrer l'*épaisseur pluristratifiée* de chaque problématique. Impératifs qui conduisent encore à saisir l'importance du *milieu*, à *contextualiser* les faits à leur environnement, à *élargir le spectre d'exploration* en vue de saisir le plus grand nombre d'éléments et de relations en jeu, à dégager les multiples *ramifications* à l'œuvre dans chaque configuration : « Quel que soit le sujet considéré, et quel que soit l'esprit qui le considère, la question de lieu ou de milieu doit toujours être posée⁵. »

Développer des analyses fondées sur des instruments de *captation* variés consiste encore à refuser des formules à l'emporte-pièce supposées circonscrire un phénomène. La fameuse assertion de Deleuze « déclarant » le passage de la société disciplinaire à la société de contrôle n'est certes pas tendanciellement fausse, mais occulte par sa force de quasi-slogan la pluralité des structures en jeu. Le contrôle en tant que tel représente un concept vide qui ne renvoie à rien de précis, ou qui renvoie plutôt, par sa pure abstraction, exactement à ce qui relève du *fantasme*, déterminé par l'ignorance et la peur. J'affirme ici qu'il n'existe pas de société placée sous emprise absolue, car ce serait croire possible une « manipulation » radicale et définitive des personnes ; ces « opinions » sont fondées sur le postulat de la dimension majoritairement passive des singularités, sur le préalable inconséquent et naïf de la victimisation des individus relativement aux supposées « forces occultes du pouvoir ».

C'est ignorer d'abord la force de chacun à *recomposer*, à reconstruire chaque situation ; à ce sujet les remarquables analyses de Michel de Certeau sur les capacités de réappropriation individuelle, les usages propres, les *tactiques* et *ruses* singulières, n'ont probablement pas été suffisamment reçues⁶. C'est ignorer encore la quantité de « trous » qui affaiblissent les « maillages ». Une infinité d'événements *échappent*, et repoussent *de facto* toute perception massive et close des phénomènes. Si nous étions dans une société de contrôle, nous pourrions approcher du « risque zéro ». Si nous étions dans une société de contrôle, les attentats du 11 septembre 2001 aux

États-Unis, du 11 mars 2004 à Madrid, de juillet 2005 à Londres, ne seraient pas advenus, les traces auraient été repérées ; or ce qu'exposent ces impacts inattendus, c'est précisément la profusion de « cases vides ». En revanche, la « société du risque » concourt à étendre selon des mesures inouïes des dispositifs de surveillance presque omniprésents. Mais « contrôle » et « surveillance » constituent deux notions différentes, l'une ambitionne vainement d'orienter les individus, l'autre de *recueillir* des informations à leur sujet ; chacune renvoie à des illusions ou à des efficacités distinctes.

Trop d'appréciations sont fondées sur des logiques binaires, modalités qui devraient définitivement appartenir à des comportements historiques révolus. Les « surveillants » ne sont pas situés d'un côté et les « surveillés » de l'autre, nous verrons que le statut des uns et des autres glisse en permanence, ce qui rend la situation si fluctuante et abyssale. Certes, quantité de machines d'observation prolifèrent, mais elles restent *fragmentées*, et tant que la plupart d'entre elles ne seront pas reliées, « agrégées », alors la figure omnipotente de « Big Brother » s'exposera comme une chimère patente d'ignorance aveugle à une cartographie polymorphe des réalités. Enfin, la représentation du « contrôle » n'est jamais très éloignée de l'illusion de la « théorie du complot », qui voudrait percevoir l'ensemble des faits « manœuvré » par des forces « masquées ». Un des pires maux de l'époque consiste à entretenir et à diffuser des formules simplificatrices, à un moment de l'histoire traversé par des problématiques d'une extrême complexité, laquelle requiert des efforts d'analyse aptes à balayer et à faire pivoter la *multitude* des éléments hétérogènes qui composent les situations autant que les jeux manifestes ou plus discrets de leurs interactions.

Un des enjeux de cet ouvrage consisterait encore à développer une posture active, à encourager des *processus de subjectivation*, à s'opposer à l'idée reçue selon laquelle la grande majorité serait le « jouet » d'une minorité qui contribuerait, pour toute une série de raisons, à instaurer un environnement inquiétant. Il pourrait formaliser un effort de *réappropriation*, à l'instar de propositions artistiques décidées à déjouer, rejouer, exemplifier certaines situations à l'œuvre. Cette enquête s'inscrit dans le cadre d'un « laboratoire de recherche » que je mets en place, qui vise à contextualiser mes travaux d'écriture à l'intérieur d'un environnement technico-culturel caractérisé par une transformation de nos rapports à la textualité, en partie due à l'apparition et à la généralisation de nouveaux supports, qui favorisent en outre la prolifération exponentielle de messages et de codes numériques – toujours plus soumis à des procédures de surveillance. À mon sens, les flux instables tracés par la société de l'information du XXI^e siècle constituent un *champ d'exploration littéraire* privilégié, qui appelle à se confronter aux mutations présentes et à venir qui frappent les conditions de l'*écrit* et à développer des stratégies de recherche *multimodales*, aptes à *superposer* et entrecroiser corpus théoriques et poétiques.

Les axes méthodologiques déployés ici visent à se soucier d'une nécessaire mise en perspective historique, à évaluer des *cas de figure*⁷ et non pas des généralités, à être capable de gérer des contradictions et non pas de les occulter au profit de la synthèse ou de l'inclination idéologique, à saisir la nature fortement *composite* des problématiques et incidences en jeu, d'ordre *technique, économique, politique, social, juridique, éthique, culturel, esthétique*. Notre entreprise envisage l'exploration du champ de la surveillance comme un *prisme d'observation privilégié* de notre *environnement contemporain*, en la tenant pour un enjeu majeur de notre temps : « Prenons garde d'entrer dans l'avenir à reculons » (Paul Valéry). Le projet suppose enfin d'entrelacer des modes d'approche variés : *descriptions, analyses, hypothèses, projections*, à l'intérieur d'une *recherche pluristratifiée*, de nature philosophique et à portée *anthropologique*.

1- « Une économie de consommation doit aussi être une économie d'objets à vieillissement rapide, une obsolescence quasi instantanée, et de la rotation des biens » (Zygmunt Bauman, *La Vie liquide*, Rodez, Le Rouergue/Chambon, 2006, p. 36).

2- Ce qui est nommé « Web 2.0 », « Web 3.0 »... Et leurs développements futurs ne feront qu'accroître les échanges horizontaux entre individus ; la prolifération des blogs et des espaces dits « communautaires » est emblématique de ces nouvelles formes communicationnelles et relationnelles.

3- Par exemple, la vitesse avec laquelle a été adopté l'arsenal juridique nommé Patriot Act, voté en octobre 2001, six semaines seulement après le 11 septembre. Sur cette question, cf. Robert Harvey et Hélène Violat, *USA Patriot Act, de l'exception à la règle*, Paris, Éditions Lignes, 2006.

4- Paul Valéry, *Regards sur le monde actuel et autres essais*, Paris, Gallimard, « Folio essais », 1933, p. 281.

5- *Ibid.*

6- Cf. Michel de Certeau, *L'Invention du quotidien. Arts de faire*, Paris, Gallimard, 1990.

7- « Tous les phénomènes sont singuliers, tout fait historique ou sociologique est une singularité ; Foucault pense qu'il n'existe pas de vérité générale » (Paul Veyne, *Foucault. Sa pensée, sa personne*, Paris, Albin Michel, 2008, p. 22).

I

INTERCONNEXION

Maillage électronique intégral

Un monde interconnecté

Un événement technologique capital s'est développé depuis une cinquantaine d'années suivant un rythme exponentiel : celui de l'extension du numérique, qui s'est fortement accélérée au cours des années quatre-vingt, et qui a progressivement investi un nombre grandissant d'objets. L'usage de l'ordinateur a d'abord inscrit l'écrit comme le résultat de calculs ; ensuite l'apparition des CD audio a rendu manifeste la digitalisation d'autres types de données. La production d'appareils photo et de caméras numériques a confirmé l'étendue du phénomène, simultanément à l'introduction généralisée et sans cesse croissante de quantité de puces électroniques dans de nombreuses strates de notre environnement quotidien. Parallèlement, les réseaux de télécommunication ont recouvert une portée « globale », grâce à l'extension des nœuds d'émission et de réception (antennes, câbles, fibres optiques, satellites), à l'augmentation des vitesses de débit et à un perfectionnement des techniques de gestion et de traitement des flux électroniques. La planète est désormais entièrement *quadrillée* par des relais de transmission qui relient la totalité de ses surfaces, à l'intérieur d'une sphère universelle toujours plus « compressée » par les filaments qui la structurent et les dons d'instantanéité qu'ils autorisent.

D'une certaine façon, ces deux phénomènes majeurs sont sans rapport entre eux (bien qu'ils aient chacun mutuellement bénéficié des avancées de l'un ou de l'autre). Ils constituent deux branches bien distinctes de l'histoire de la technique, dans la mesure où n'a jamais été consciemment et volontairement « programmé » un des événements parmi les plus décisifs de notre temps : la *conjonction* systématisée et standardisée du numérique et des réseaux de télécommunication. Internet représente le dispositif le plus emblématique issu de ce « tissage » imprévu, et constitue le protocole majeur destiné à recevoir, percevoir et diffuser des données informationnelles. Une quantité toujours plus importante d'objets est structurée selon une

configuration interconnectée : ordinateurs, téléphones portables, organisateurs personnels, lecteurs MP3... La dimension numérique induit la réduction de données hétérogènes (écrit, son, image fixe et animée) à des codes binaires identiques, qui autorise la manipulation de régimes symboliques distincts à l'intérieur d'un même « environnement » et à l'aide d'une même interface : clavier, touches, pression tactile, commande vocale... Instruments *en réseau* devenus ordinaires dans la quotidienneté offrant des usages multiples et mobiles, qui rendent tendanciellement possibles des procédures de surveillance élargies et inédites – autant « verticales » (d'organismes vers les personnes) qu'« horizontales » (personnes entre elles). L'*interconnexion* dans sa configuration actuelle permet non seulement de saisir ou de transmettre différents types de données mais encore de *géolocaliser* corps, objets et espaces ; en outre, le nombre de protocoles *sensibles* ne cesse de suivre des courbes de progression astronomique, situant l'*individu hypermoderne* à l'intérieur d'une *maille* virtuelle aux filaments continûment resserrés et aux modalités de « capture » toujours plus répandues, simplifiées et sophistiquées.

L'association entre numérique, réseaux de télécommunication et *intelligence artificielle* a favorisé la gigantesque mise en place de *bases de données* (sur lesquelles nous reviendrons), qui représentent la part emblématique d'une application de l'interconnexion, capitalisée en vue de dresser des *cartographies individualisées* et *indexées* des corps et des usages. L'*interconnexion* amplifie les pouvoirs de la surveillance, selon des degrés de facilité, de rapidité, d'efficacité jamais connus dans l'histoire. Un nombre sans cesse croissant d'objets dotés de structures connectées contribue non plus seulement à ce que les individus communiquent entre eux au moyen de ces technologies, mais à ce qu'il s'opère une *mise en relation continue* des unités matérielles entre elles : ce qui est nommé l'« Internet des objets », qui constitue une évolution du Web et un « saut » dans la perspective du « tout connecté ». Les communications s'opèrent via des adresses IP (câbles ou Wi-Fi) ou des étiquettes électroniques (RFID, sur lesquelles nous reviendrons également), liaisons *sans fil* en *interaction* permanente qui impriment une sorte de « rythme vital » aux *processus relationnels* entre les choses.

Le corps/interface

Plus encore, il se dessine l'horizon d'un large *spectre communicationnel* qui reliera continuellement individus entre eux, objets entre eux, individus et objets, dans un milieu marqué par l'interactivité ininterrompue des corps et des surfaces (choses et espaces physiques), induisant quantité de *variations* environnementales (température, luminosité, gammes chromatiques...), rendues possibles par la présence de capteurs et l'introduction de puces dans les corps, qui établiront des équations – décisions paramétriques offertes par les logiciels –, configurant en temps réel les tensions entre personnes et qualités des atmosphères. Ces tissages se forment peu à peu selon une

dimension devenue capitale du design contemporain : celle d'*intégration*, qui vise à *fondre* des données hétérogènes (nouveaux matériaux et composants électroniques) à l'intérieur d'un même *plan*, en vue d'implanter des *systèmes communicants*. La surveillance contemporaine s'inscrit déjà et va sans cesse se développer au sein de ce complexe, qui assimile entre elles données matérielles et numériques. Le mouvement historique d'entrelacement progressif entre physique et virtuel¹ produit de nouvelles surfaces *pluristratifiées*, unifiées dans des armatures communes, qui vont faciliter l'*incorporation* des structures de surveillance selon des dispositifs rendus toujours plus *invisibles* dans l'environnement. La série prémonitoire *Le Prisonnier* (1967), conçue et réalisée par Patrick McGoochan, expose un village entièrement quadrillé par des techniques de suivi des corps ; le maître des lieux – nommé Numéro 1 – ne se manifeste jamais physiquement, comme le signe patent de son omnipotence toujours confirmée par son absence et qui amplifie la paranoïa relative à l'étendue de son acuité ou de ses pouvoirs.

Les développements à venir des *nanotechnologies* intensifieront la puissance d'*intégration* – non pas tant en termes de fusion toujours plus fine que par des procédures d'articulation entre éléments distincts composées selon une échelle inusitée à ce jour : celle de l'atome. N'importe quelle minuscule unité sera susceptible d'être formée et traitée suivant des paramètres spécifiques, à côté d'autres particules tout autant singulières, faisant du *nombre* et de la *différence* non plus seulement l'ordre de la « nature », mais celui de notre biosphère artificielle, tissée de *matrices différentielles* continues. Par extension, cet investissement de l'*infiniment petit* (à coup sûr un des axes majeurs de la recherche du XXI^e siècle) appelle à déployer une structure de pensée et une approche méthodologique, fondées sur une « particularisation » des perceptions, des modalités d'analyses et des axes constructifs, conscients du fractionnement, de la *singularité* et de la *mobilité* de chaque enjeu et problématique, à l'écart de toute synthèse réductrice. Semble dorénavant poindre une « divulgation sensible » de certaines lois physiques majeures du XX^e siècle (mécanique quantique, théorie de la relativité, du chaos, de la complexité...) rendues maintenant *manifestes* dans les faits. Cette *cinématique* du réel, cette énergie du visible, depuis longtemps théorisée – désormais « palpable » –, constitue un événement technique et anthropologique capital du XXI^e siècle, susceptible de défaire nos catégories historiques fixées sur l'*identité* et la *stabilité*. Il se dégage ici une interrogation d'ordre philosophique, cognitif, culturel, comportemental : celle de nos capacités à *modifier* nos schémas conceptuels ancestraux, pour la plupart inopérants à se confronter activement aux surfaces de notre hypermodernité sans cesse mouvante, infiniment et indéfiniment fragmentée, et désormais appelée à être « nano-manipulée ».

L'interconnexion ne constitue pas un événement technologique parmi d'autres, elle ne représente pas à proprement parler une *technique* (qui

viendrait se substituer à une plus ancienne, et qui rapidement serait suppléée par une autre, davantage perfectionnée), mais dessine plutôt une « superarchitecture universelle » aux contours évolutifs, ouverte à une infinité de protocoles présents et à venir. (À l'instar des routes, qui ne sont pas des techniques, mais un ensemble de virtualités matérielles qui ont transformé les rapports historiques entre individus, communautés, territoires, ou encore à l'instar du transport aérien de masse, qui ne forme pas non plus une technique, mais désigne un vaste ensemble en constante mutation, qui a redessiné et compressé une cartographie planétaire historiquement sillonnée par les voix terrestres ou navigables.) Étant donné l'étendue que l'*interconnexion* a prise depuis l'avènement d'Internet, les multiples applications qu'elle permet (aux incidences innombrables dans les champs scientifiques, industriels, économiques, culturels, et dans quantité d'activités du quotidien), elle relève d'une nouvelle *dimension anthropologique*, dans la mesure où elle affecte, selon des mesures sans précédent historique, les conditions de l'expérience : les relations ancestrales à l'espace et au temps. Ce que nous connaissons et éprouvons aujourd'hui de ses pouvoirs renvoie prioritairement à la possibilité récente d'effectuer quantité d'opérations à distance, selon une sorte de don d'ubiquité partagé ; cependant cette faculté ne représente désormais qu'une partie de ses propriétés. Le *corps* s'annonce comme l'unité centrale, située au point de convergence entre faisceaux de connexions, capteurs et serveurs, au sein d'une étape ultérieure de l'*interconnexion*, se déployant non plus par des décisions prises via des interfaces, mais par le résultat de tensions continues entre individus et espaces, sous forme de gigantesques puissances de calculs, de transmissions, et d'analyse des données, exposant des architectures réactives et instables, reliées à des êtres – organes de chair – toujours plus *accessibles et transparents*.

Néanmoins cette ossature globale n'offre pas une « robustesse » entièrement garantie, elle revêt une fragilité qui fait peser une menace permanente sur les systèmes. D'abord, parce que les codes numériques ne fournissent pas d'original, de trace initiale attestant de l'authenticité d'un document, qu'ils sont au contraire susceptibles d'être aisément reproduits, dupliqués à l'infini. En outre, malgré certaines procédures d'encryptage, ils peuvent être interceptés sur les réseaux et utilisés à des fins délictueuses. Ils rendent également possibles des « attaques » – infiltration frauduleuse dans les serveurs, modification des données, propagation de virus – capables de perturber ou de détruire les architectures électroniques. L'ensemble de ces *failles* expose un « paradoxe numérique » : un hiatus entre une armature générale qui semble solide, rapide, efficace, et dont on sait cependant qu'elle repose sur une sorte de « château de cartes » – instable fondation informationnelle universelle.

La fameuse crainte du « bug de l'an 2000 », son ampleur, les procédures et précautions qu'elle a occasionnées – finalement en pure perte –, ont manifesté

un rapport au numérique fondé sur une large part impulsive et irrationnelle (cette « perfection » aurait nécessairement un envers périlleux, peut-être fatal ; rappelons qu'avait été évoquée à l'époque l'hypothèse de crashes aériens, de dérèglement des échanges bancaires ou des cotations boursières...). Il est apparu dans le même mouvement une nouvelle conscience de la *vulnérabilité* des systèmes, des périls qu'ils seraient susceptibles de faire courir à l'égard d'enjeux décisifs (économiques, financiers, militaires, sécuritaires...), à tel point que le principe de la *sécurisation des réseaux*² représente une dimension majeure de la surveillance contemporaine. Le spectre du risque encourage une surveillance des systèmes – notamment ceux de surveillance – suivant des enchaînements en spirale où des réseaux sont chargés de surveiller des réseaux eux-mêmes chargés de surveiller... Toutefois, l'interconnexion ne renvoie pas à un ensemble homogène mais à une *infinité* de structures plus ou moins reliées, pour la plupart indépendantes les unes des autres, rendant dans les faits impossible le risque d'un bug global – illusion fondée sur l'unité des dispositifs –, alors que ce sont le *nombre* et la *dispersion* qui catégorisent notre moment historique.

1- « Physique/virtuel » est le titre d'un colloque que j'avais organisé à la médiathèque d'Orléans en mai 2005, dont l'objet consistait à explorer la nature et la portée des entrelacements croissants entre espaces, corps et protocoles de computation *intégrés*.

2- Thales, par exemple, est devenue au fil du temps une entreprise globale – 60 000 salariés présents dans cinquante pays –, experte dans les « solutions de sécurisation des réseaux ».

II GÉOLOCALISATION

Perception extra-atmosphérique hors- mesure

Quadrillage universel

Désormais l'*interconnexion* est indissociable de la *géolocalisation* : procédure de repérage et d'identification des corps et des choses – équipés de puces adéquates –, qui émettent un *signal* à l'adresse de robots électroniques, ou visibles sur des cartes virtuelles. Il se déploie un nouveau « panoptisme planétaire », chargé non plus, à l'instar du *Panopticon* de Jeremy Bentham, de résoudre au mieux l'équation entre moyens humains et efficacité de la surveillance des prisonniers, mais de situer les individus sur des « abscisses électroniques », à l'intérieur d'un *quadrillage* systématisé dépourvu de « trous », par le fait de la couverture satellitaire *globale*. Le premier dispositif standardisé et universel, le GPS américain, a rendu possibles la fiabilité et la généralisation de la géolocalisation, laquelle répondait à l'origine à une exigence militaire, celle de pouvoir repérer les unités en mouvement (flottes maritime et aérienne, forces terrestres). Plus loin dans l'histoire, ce mécanisme doit à la capacité scientifique de lancer régulièrement, depuis la fin des années cinquante, des satellites géostationnaires qui peu à peu ont été remplacés par d'autres appareils, plus sensibles aux fréquences de réception et plus aptes à renvoyer les signaux.

Une date importante – inaugurale de l'ère spatiale – a concouru à ce que les États-Unis, constatant leur vulnérabilité, accélèrent leur programme systématique de lancement : le 4 octobre 1957, l'Union soviétique mit *Spoutnik* sur orbite et manifesta une maîtrise nouvelle des missiles balistiques intercontinentaux. Cet événement déclencha une psychose politique et militaire sous l'expression de *Missile Gap*, qui encouragea le déploiement des premiers moyens spatiaux d'alerte, d'observation et d'écoute, accordant une nouvelle priorité à la surveillance satellitaire, et que toutes les administrations successives, sans exception, s'attachèrent à développer. La fameuse « guerre des étoiles » initiée par Ronald Reagan (IDS, Initiative de défense

stratégique), qui visait la mise en place d'un *bouclier virtuel* apte à signaler et à interrompre toute course de missile, s'inscrit au cœur de cette histoire, autant que les dispositifs miniaturisés de géolocalisation portés par les soldats lors de la guerre du Golfe en 1991¹, au sujet desquels la chaîne d'information en continu CNN réalisa à l'époque quantité de reportages à l'attention de téléspectateurs surpris par la réalité et l'efficacité de technologies portables reliées à l'espace.

À la fin des années quatre-vingt-dix, les États-Unis décidèrent de mettre en place une toute nouvelle architecture militaro-spatiale, dont l'objectif – par la suite amplifié et légitimé par les événements du 11 septembre 2001 – ambitionnait de garantir une domination sur l'« étendue extra-atmosphérique ». Ce processus formalisé par le Pentagone sous la formule explicite de *Space Power* conduisit à une progressive militarisation de l'espace orbital. Il a, par exemple, encouragé l'organisation et la réalisation par le Space Warfare Center d'une gigantesque simulation d'un conflit visant les satellites, une sorte de premier « *wargame* spatial » (*Schriever 2016*), ou encore le futur déploiement stratosphérique d'armes à énergie cinétique antisatellites. Cette axiomatique structure le projet de *Future Imagery Architecture* dirigé par le NRO (National Reconnaissance Office), qui consiste à concevoir des satellites espions, plus légers et plus puissants, non plus seulement capables de visionner avec toujours davantage de précision les territoires, mais de les « interpréter » en temps réel, de saisir un nombre beaucoup plus important d'informations et de les traiter à l'aide de bases de données embarquées et de transmission à d'autres bases de données situées au sol, selon des paramètres d'analyse évolutifs. La nouvelle fonction des systèmes satellitaires ne consiste plus à avertir d'une localisation mais à opérer un acte d'*interprétation* d'un composé d'éléments, non plus seulement à signaler une présence, mais à réaliser des procédures d'*expertise robotisée*. « Au début du XXI^e siècle, nous serons capables de trouver, suivre et cibler en quasi-temps réel n'importe quel élément d'importance en mouvement à la surface de la Terre, à l'aide de capteurs chargés de déceler toutes sortes de vibrations, acoustiques, gravimétriques, chimiques, sismiques, thermiques, dans le visible, l'infrarouge et l'ultraviolet, dans de très larges segments du spectre électromagnétique, radar, sonar, détecteurs d'anomalies électromagnétiques, signaux hertziens..., grâce à la couverture satellitaire et aux puissances d'analyse en temps réel », annonçait dès 1997 le chef d'état-major de l'US Air Force.

La volonté de plusieurs pays de se doter de capacités de reconnaissance satellitaire incita les États-Unis en 1994 à autoriser l'utilisation commerciale de l'imagerie métrique, façon de devancer et de neutraliser toute velléité concurrentielle potentielle. En 1996 fut instaurée la National Imagery and Mapping Agency (NIMA), organe du département de la Défense chargé de l'exploitation des images, de la cartographie militaire et du soutien aux

activités industrielles. Une longue histoire du transfert de technologies militaires vers le civil, favorisé par une volonté politique et économique, caractérise une *pragmatique* américaine de la synergie. Par exemple, les relations entre le développement d'une force aérienne militaire et l'aéronautique civile ont été particulièrement étroites aux États-Unis alors qu'elles ont été plus distendues dans les pays européens. Les appareils commerciaux qui ont assuré la suprématie des constructeurs américains ont directement bénéficié de programmes financés sur fonds publics. Plusieurs exemples démontrent l'étroitesse de ces liens : le Boeing 707 conçu dans les années cinquante a été le premier avion de ligne à quasiment monopoliser le marché tout au long des années soixante. Près de 90 % de son système et de ses composants provenaient de développements militaires : les apports les plus importants étaient issus des bombardiers B-47 et B-52.

La passion proprement américaine pour l'innovation s'est en partie épanouie par le fait d'une mise en réseau systématique entre puissances hétérogènes : armée, universités, compagnies privées, groupes financiers (capital-risque), qui a notamment produit le succès le plus emblématique de cet « esprit coopératif », celui de la Silicon Valley. Par exemple, le concept de « *dual use* » aspire autant à l'utilisation par les unités militaires de systèmes civils qu'à l'inverse sous certaines conditions. Laurent Muraviec, analyste auprès du *think tank* californien Rand Corporation, affirmait que « l'innovation change le visage de la guerre, ce qui suppose une révolution dans les affaires militaires² » que les stratèges du Pentagone nomment « *guerre de la connaissance* », celle qui vise à développer des technologies sophistiquées de « pénétration informationnelle », cœur d'une stratégie autant destinée à remporter des batailles économiques que les conflits dits *asymétriques* ou de *basse intensité*.

Internet, qui favorise jeux d'échanges horizontaux, projets artistiques et culturels, utopies plus ou moins fondées, tout autant que l'apparition et le développement de nouveaux géants économiques, trouve son origine dans un projet militaire : à la fin des années cinquante, durant la guerre froide, le département de la Défense crée l'*Advanced Research Project Agency* (ARPA), dont l'objectif consiste à établir la juste parade à un cas de figure précis : comment maintenir les télécommunications après une attaque nucléaire ? Militaires, informaticiens, universitaires conçoivent après dix années de travaux un protocole dont le nom n'est pas encore Internet mais *ARPAnet*, qui relie pour la première fois en 1969 quatre campus américains qui peuvent transférer leurs données sur un réseau commun. Charles Wilson, P-DG de General Motors pendant la Seconde Guerre mondiale, considérait qu'il n'y avait pas de « différence entre les bénéfices de l'entreprise et les intérêts du pays », conformément à une perception communément partagée qui conduit encore à ce que des réunions régulières se tiennent à la Maison-Blanche, dans la *War Room*³, comprenant responsables politiques, militaires, scientifiques,

économiques, dont l'objectif vise l'élaboration de stratégies commerciales entendues comme des *tactiques de guerre*, notamment par la surveillance des communications, la collecte d'informations relatives aux projets de recherche et de développement menés au sein d'entreprises étrangères, à leurs programmes de vente, à des négociations en cours⁴...

La cible majeure pointée par ces associations transversales concerne le *renseignement*, arme décisive du XXI^e siècle, à la *force de frappe* multiple, notamment industrielle. Collaborations aux intérêts *conjoint*s, capables de pousser les élus du peuple à fléchir face aux arguments de préservation des emplois nationaux et à succomber aux gigantesques pressions financières. En 1961, le général Eisenhower, dans son remarquable discours d'adieu, avait mis en garde les démocraties contre la puissance du complexe militaro-industriel, susceptible de menacer leur assise fragile et l'intégrité des gouvernements : « Cette conjonction d'une immense institution militaire et d'une grande industrie de l'armement est nouvelle dans l'expérience américaine. Nous reconnaissons le besoin impératif de ce développement. Mais nous ne devons pas manquer de comprendre ses graves implications. Le risque potentiel d'une désastreuse ascension d'un pouvoir illégitime existe et persistera. Nous ne devons jamais laisser le poids de cette combinaison mettre en danger nos libertés et nos processus démocratiques. Seule une communauté de citoyens prompts à la réaction et bien informés pourra imposer un véritable entrelacement de l'énorme machinerie industrielle et militaire de la défense avec nos méthodes et nos buts pacifiques, de telle sorte que sécurité et liberté puissent prospérer ensemble⁵. »

Ces entrecroisements industriellement fructueux mais politiquement inquiétants n'ont pu être historiquement développés par l'ex-URSS (absence de pouvoir économique), par le Japon (absence de pouvoir militaire) ou par l'Europe (sanctuarisation de l'armée, de sa valeur jugée « secrète », strictement réservée et protégée, dimension particulièrement manifeste en France, où les modes d'organisation ont toujours été marqués par les principes de *hiérarchisation* [jacobinisme] et de *séparation* [cartésianisme]). En 1985, Robert Reich, futur secrétaire au Travail de Bill Clinton, affirmait : « La guerre des étoiles n'a été qu'accessoirement pensée dans un but de défense nationale, sa fonction principale a été d'ouvrir une voie vers la compétitivité dans les hautes technologies » ; constat qui conduit certains, comme Seymour Melman⁶, à militer pour le *Conversion Project*, qui consiste à favoriser les conditions possibles de report des gigantesques sommes allouées aux dépenses militaires, ainsi que les hautes qualifications des équipes, appelées désormais à être affectées à de nouvelles activités à dimension éthique, celles favorisant notamment le développement durable, les soucis écologiques, les sources d'énergie du futur... Ce positionnement trouve sa légitimation dans l'hypothèse d'une conversion historique, à terme inévitable, au vue de la diminution des conflits mondiaux⁷. Néanmoins ce « combat » évidemment

honorable ignore les structures de la guerre du XXI^e siècle, de plus en plus configurée par l'engagement de forces sur des territoires éloignés (missions humanitaires, opérations commando, interventions « préventives », qui toutes nécessitent de puissantes machines de renseignement)⁸.

La plus grande légèreté des unités ne suppose pas une diminution des budgets mais une sophistication des techniques et des équipements qui requiert des investissements de recherche et de développement considérables, dont les productions revêtent pour la plupart une substance « immatérielle » : systèmes de communication, de vision, d'interopérabilité des dispositifs, constitution de bases de données..., qui certes n'imposent pas l'allure impressionnante d'armes conventionnelles, mais qui représentent le résultat quasi invisible de programmes coûteux, de surcroît sans cesse appelés à être renouvelés par le fait de la techno-temporalité qui induit des processus de mutabilité exponentielle – propres au XXI^e siècle. C'est aussi ignorer à quel point aux États-Unis, tout comme en Europe, armée et pouvoir politique sont traditionnellement liés – presque « ligüés » –, non par une intrication indémêlable comme ce fut le cas dans les dictatures sud-américaines au cours des années soixante-dix, mais au nom de l'exigence de protection qu'un État démocratique se doit de garantir à l'égard d'ennemis extérieurs. Cet impératif est entendu comme une dimension politique constitutive et essentielle, qui a *de facto* délégitimé les velléités antimilitaristes successives, et ce à l'intérieur d'un consensus généralisé droite/ gauche. C'est encore au nom de ce principe que les États-Unis s'investissent autant dans la lutte antiterroriste, à coup sûr pour de multiples autres raisons et intérêts entrelacés (le discours d'Eisenhower rappelait l'impératif de vigilance à l'encontre de l'influence sournoise de l'industrie militaire) ; néanmoins c'est prioritairement au nom de cet axiome jugé indéfectible – aux nombreuses conséquences géopolitiques, éthiques, juridiques – que la « guerre contre la terreur » représente depuis le 11 septembre 2001, à tort ou à raison, la première priorité politique du pays.

Il faut relever que dans le cadre de la relation complexe qui associe pouvoirs militaires et économiques, ou dans celui du « transfert technologique » vers le civil, de nombreux protocoles initialement conçus à l'intention des forces armées – notamment certains dispositifs de surveillance – se sont trouvés délégués à des entreprises privées, et par la généralisation de leurs produits se sont encore retrouvés pour certains d'entre eux à la portée de *tous*. C'est le cas d'Internet (qui, nous le verrons, autorise quantité de procédures de surveillance – évidemment par les organes d'État : police, sécurité intérieure..., mais tout autant, quoique selon des visées distinctes, par le marketing contemporain ou par les individus entre eux). C'est encore le cas de certaines techniques biométriques ou certains programmes de reconnaissance des visages et des formes. C'est enfin le cas, nous l'avons vu, de la géolocalisation. De nombreuses innovations militaires chargées de prévenir, détecter, situer, ont fait l'objet de développements

ultérieurs au sein de laboratoires civils, dont les produits ont été mis sur le marché, destinés à d'autres usages, mais qui ont finalement recouvert pour partie leur fonction initiale – comme un retour du refoulé –, déployée non plus à l'intérieur d'un champ de bataille virtuel mais dans le champ de la socialité, favorisant une augmentation généralisée des capacités collectives et individuelles de surveillance.

À l'inverse, on peut constater la récupération par les militaires d'innovations issues du civil, à l'exemple des jeux vidéo en vue de développer des scénarios de simulation ou de stimuler les capacités de réactivité, selon des jeux de « recyclage » entre champs hétérogènes qui engagent des utilisations inattendues, par effets de *recontextualisation* qui signalent à quel point chaque protocole est disposé, autant que possible, à offrir des applications initialement imprévues dans les programmes initiaux. La *technique*, contrairement aux clichés trop répandus, ne constitue jamais une force qui impose, mais une puissance qui *propose*, au nom de la faculté proprement humaine à se *réapproprier* les objets, à rejouer les fonctions et les relations, selon des configurations qui jamais ne se confondent exactement avec le *mode d'emploi* originaire⁹.

À coup sûr ne relève pas du hasard le fait qu'à l'intérieur de notre environnement épistémologique, marqué par la multiplicité, le nombre, le foisonnement, s'épanouisse une tendance artistique majeure qui consiste à jouer et à composer avec quantité de *sources*, à envisager les particules constitutives de la pluralité comme formant autant d'ensembles mouvants et disponibles, *bases de données* ouvertes à une infinité de procédures combinatoires ; phénomène emblématique dans le DJing. Une disposition ici se développe qui souhaite négocier avec l'« existant », capable de transformer des plans reconnaissables en des figures inédites. L'étendue croissante des structures de surveillance offre notamment aux pratiques artistiques l'occasion d'investir un champ d'exploration aux multiples enjeux et de se confronter à des technologies sophistiquées (capteurs, systèmes d'analyse et de détection, protocoles de transmission...). Usages et fonctions sont susceptibles d'être exemplifiés, intensifiés, déjoués dans l'espace public ou privé. Apparaît la perspective de mise en place de dispositifs non encore élaborés, à l'efficacité infaillible, ou à la dimension effrayante ou inutile, qui tous ont le mérite de requérir l'expérience, l'implication des corps, et d'exposer *visiblement*, et *de biais*, des formations à l'œuvre dans l'environnement, celles-ci souvent *dissimulées*, réellement intrusives, et ne relevant pas, pour leur part, de la « fiction ».

L'aptitude à recombinaison et à rejouer objets et situations recouvre une portée éthique et esthétique en ce qu'elle témoigne d'un effort de *subjectivation* qui affirme le pouvoir de *plier* autrement une production, non en vue d'asseoir une maîtrise, mais dans l'objectif d'exposer le *maniement singulier* comme étant irréductible à toute fonction *a priori* (dont l'exemple, certes dérisoire, de la *customisation* serait emblématique d'une forme de

conscience somme toute discrète de cette possibilité). Plus largement, cette *liberté* regarde l'*écart* irréductible qui sépare phénomènes massifs et individu autonome, à la fois partie de la communauté et être d'*exception*, structurellement situé à *distance*, dont les *virtualités* ne peuvent jamais être réduites à la somme des équations collectives. L'extension des procédures de surveillance peut en partie être *troublée* par des stratégies individuelles ou collectives structurées et informées, qu'elles soient d'ordre artistique ou d'usage (refus d'activer certaines fonctionnalités, par exemple). Jeux d'*invention* et actes d'*innovation* déployés comme autant de cellules actives capables de *redessiner* les structures existantes, d'affaiblir certains de leurs pouvoirs ou de leur octroyer d'*autres qualités* jusque-là enfouies.

Clairvoyance panosphérique

Le principe d'une délégation d'un programme militaire à l'attention d'opérateurs civils, apte à favoriser l'éclosion de quantité de nouveaux usages, est particulièrement manifeste dans le cadre précis du GPS. En 1994, la décision prise par l'administration Clinton d'autoriser un usage commercial du système permit la mise en place de nombreuses applications. Depuis, un nombre sans cesse croissant de véhicules sont équipés de navigateurs qui gèrent les itinéraires et fournissent des informations relatives au trafic. Les avions de transport utilisent la constellation satellitaire pour tracer leur route ou négocier les atterrissages sous pilote automatique. Navires, trains, camions, taxis sont désormais dotés de récepteurs, assurant un positionnement identifié en continu et une gestion optimisée des flux. Le GPS assure encore la navigation dans les ports ou l'emplacement des plates-formes de forage au centimètre près, à tel point que le principe de la localisation des corps et des choses sur un plan ne s'opère plus à l'intérieur d'une « immanence » incontournable, selon des repères toujours situés historiquement « au ras du sol », mais selon un nouvel « aplomb » universel, établi dans l'atmosphère, et qui contredit en partie les propositions de la phénoménologie husserlienne qui affirment l'impossibilité d'une vision globalisante des choses. La couverture satellitaire contribue à perturber une sorte d'égalité *partagée* et ancestrale de la capacité humaine à restreindre son champ de représentation à la perspective imposée par la *mesure du corps*, et dont les techniques d'amplification de la vision élaborées jusque-là constituaient seulement des *prothèses* restreintes qui s'inscrivaient à l'intérieur de la même *proportion*.

Probablement sommes-nous passés du fantasme de la « vision panoptique » (crainte chimérique, autant qu'objectif à atteindre, irréalisable dans les faits¹⁰) à la réalité d'une « perception extra-atmosphérique », au spectre optique global, mais non intégral, et ce pour deux raisons. La première veut qu'à ce jour, une majorité d'objets et de corps ne sont pas dotés de puces de réception, donc ne sont pas localisables (bien que l'expansion du port de téléphones portables contredise cette réalité, mais selon d'autres modalités) ;

la seconde regarde la retenue imposée par certains cadres juridiques qui interdisent un suivi continu des individus (néanmoins cette autre réalité est sans cesse fragilisée par la nullité des frontières politiques, imperceptibles de l'espace, autant que par de nombreux vides relatifs à la surveillance par satellite dans le droit international). Nous sentons ici à quel point quantité de failles, de « trous » malgré tout demeurent dans le système et garantissent une part insaisissable à chacun de nous, et à quel point s'est opéré dans le même mouvement un « saut technologique » qui modifie notre intuition historique de la présence sur un plan, selon une portée et une efficacité *intrusives*, et qui trouble notre patiente compréhension de l'expérience construite au cours des siècles. Celle entendue comme le résultat d'une tension entre espace et temps contrainte aux sens (immanence), désormais *muée* en tant qu'*opération* quasi continue de *diffusion* et de *réception* de *signaux*, perceptible sur des *cartographies* non plus formées par les reliefs, les fleuves ou les mers, mais *calculées* d'après les *comportements* et dont les surfaces sont irriguées en profondeur par des *bases de données* évolutives plus ou moins *interconnectées*.

Une application capitale – appelée à se développer amplement – regarde l'articulation opérée entre localisation des personnes, connexion à des bases de données et proposition d'offres commerciales adaptées aux profils singularisés, situées dans la zone de présence. La gestion de la tension entre individus, territoires et habitudes de consommation traitées et archivées constitue une technique décisive du marketing contemporain, qui lui-même représente une architecture de traçage majeure de notre temps. Il se généralise un rapport à l'espace et aux déplacements physiques des corps, fondé sur la *quantification* et l'analyse statistique : « L'espace-contrôle ne passe pas tant par l'espace que par l'information. Il réduit l'espace à un simple réceptacle d'expertise numérique. [...] L'espace est évalué à travers un vocabulaire modernisé : il n'est plus composé ou visualisé géométriquement, mais calculé, calibré, estimé, prévu, optimisé¹¹. » Le suivi des véhicules se généralise (flottes de bus ou de voitures d'entreprise, par exemple), à tel point que la CNIL (Commission nationale de l'informatique et des libertés) a interdit en 2005 la mise en place par une compagnie d'assurances d'un système de géolocalisation destiné à suivre certains de ses assurés. Le mécanisme aurait permis de connaître en temps réel la position et la vitesse de ses clients, qui auraient bénéficié en cas d'accord d'une réduction de cotisation. Le corps s'expose désormais comme une *donnée*, identifiée et *traitée* en continu sur des cartographies virtuelles, dont les pratiques ne restent plus repliées à la vie privée de chacun, mais produisent des *séries de codes* stockées sur des serveurs et gérées par des puissances de calcul toujours plus aptes à affiner et à *exploiter* la somme des informations recueillies.

Il s'opère avec la géolocalisation un phénomène commun à de nombreuses techniques : un protocole initial offre plus ou moins rapidement la possibilité

d'être destiné à d'autres finalités (c'est, par exemple, le cas du rayon laser imaginé en 1917 par Einstein, qui fut jusqu'au début des années soixante un objet de recherche sans application pratique nettement définie et qui ensuite a autorisé des usages fort distincts : lecture et enregistrement de support optique numérique, mesure de distance, outils d'opération chirurgicale, télécommunications via des réseaux de fibres optiques...). Les technologies numériques interconnectées se développent particulièrement suivant ces structures en évolution différentielle, mais se caractérisent encore par le fait que la plupart d'entre elles rendent possible leur utilisation en vue de la mise en place de *fonctions de surveillance*, dans la mesure où elles constituent des puissances de captation, de réception, de traitement et de stockage informationnels. Cet axiome se fonde à l'intérieur d'une période marquée par l'universalisation de la *géo-interconnexion*, entrelacée à d'autres facteurs économiques et géopolitiques qui tous concourent, par une sorte de hasard historique, à instaurer un environnement planétaire traversé et enveloppé par une infinité de *faisceaux* de suivi et de quantification. Il est ici possible d'avancer une double affirmation d'ordre anthropologique : toute invention technique induit des conséquences *de facto imprévisibles*¹², et celles d'entre elles qui permettent virtuellement de répondre à une mission de *contrôle* sont systématiquement déployées et configurées dans la perspective de potentialiser au mieux leurs « capacités enfouies », comme une passion, profondément inscrite dans la conscience et l'inconscient humains, à fabriquer des prothèses aptes à *s'enquérir d'autrui*.

Un nouveau capteur global : Galileo

Si l'architecture satellitaire du GPS a autorisé le développement de nombreuses utilisations, pour la plupart imprévues au moment de la mise en place de la constellation, elle encourage au présent et dans l'avenir un champ de recherche industrielle parmi les plus actifs, aux perspectives d'innovation et de croissance extrêmement larges. Cette activité stratégique ne pouvait être ignorée par les Européens qui depuis 1999 travaillent à la conception de leur propre système, organisé autour de trente satellites en orbite et qui devrait être opérationnel au début de la deuxième décennie du siècle. À terme, Galileo contribuera à l'autonomie stratégique des Européens ; le système permettra notamment de guider avions de combat, sous-marins d'attaque, « missiles intelligents », chars et infanterie. Il constituera une articulation décisive au projet de « *numérisation de l'espace de bataille* » (ou pour les Américains : « *network-centric warfare* », ou encore « *opérations en réseau* »), dispositif appelé à *relier* tous les équipements armés par *intégration* des différents systèmes de capteurs et d'émission de signaux entre eux, autorisée par la couverture satellitaire. Galileo constitue d'abord un geste d'autonomie de l'Europe qui, depuis la deuxième guerre du Golfe en 2003, marque, plus ou moins nettement selon les pays, une distance à l'égard du « principe

préventif » qui prévaut dans la politique américaine de défense.

Malgré l'accord d'interopérabilité entre les deux systèmes, l'Europe s'est dotée d'un outil désormais indispensable à tous les types de conflits à venir, qui va lui permettre d'orienter et de décider ses choix tactiques dans une plus grande indépendance technologique à l'égard de l'« allié américain ». Probablement Galileo inaugure-t-il dans les faits – également symboliquement – une radicalisation de la *multipolarisation* des rapports de force qui enregistre des divergences géopolitiques, fondées sur des axiomes idéologiques distincts et parfois contradictoires. Mais il ne constitue pas seulement un système destiné aux forces armées, il représente encore un dispositif sophistiqué qui facilitera et amplifiera la mise en place de procédures de surveillance des citoyens situés sur le continent européen. Il dessine une nouvelle *couche* satellitaire, qui encouragera une accélération du nombre d'unités (corps et biens) dotées de puces d'émission et de réception de signaux, conformément à une identification systématique et expansive des individus, envisagés comme des « terminaux » sans cesse suivis à la trace, en vue de multiples « usages » – sécuritaires et commerciaux.

Les constellations de satellites permettent, outre la localisation, l'*observation* des modifications et des évolutions de certaines zones géographiques. Ce qui est nommé « imagerie satellitaire » offre des applications distinctes en fonction des différentes échelles de « vision » réglées sur les caméras. On comprend encore à quel point une même technologie autorise quantité d'usages variables, à la nuance près que dans ce cas-ci, tous concourent à renforcer l'aptitude à la « perception extra-atmosphérique », qui amplifie selon des mesures sans précédent historique la capacité, la précision et le traitement de collecte d'informations situées au sol, traçant un faisceau de *strates* au spectre global, au sein du quadrillage universel contemporain toujours plus densifié et « clairvoyant ». Gustave Flaubert écrivait : « Plus les télescopes seront parfaits, et plus les étoiles seront nombreuses¹³. » On pourrait prolonger cette assertion, fondée sur un élargissement des capacités de vision grâce aux sophistications techniques, par une autre au ton nécessairement plus inquiétant : plus les systèmes satellitaires seront « intelligents » et interopérables, plus les êtres seront suivis et quantifiés par une panoptique électronique à la précision focale et aux puissances de pénétration toujours plus démesurées.

Cette récente « clairvoyance » correspond à un fantasme ancestral, celui de pouvoir observer la Terre depuis le ciel, rêvé comme un dépassement des conditions gravitationnelles qui nous attachent au sol. Malgré sa généralisation, prioritairement à l'intention de certaines industries, ce mode de perception continue de soulever un enthousiasme, manifeste dans l'émerveillement suscité par les premières images de la planète prises de l'espace durant les années soixante, et plus récemment dans le succès des *spatiocartes numériques* (atlas géographiques définis par les données

satellitaires), ou encore de certains ouvrages photographiques exposant, suivant d'autres angles – ceux-ci aériens et non spatiaux –, les variétés topographiques des différents continents. Ce plaisir se trouve aujourd'hui stimulé par l'utilisation de nouveaux protocoles, dont le plus fameux est Google Earth, développé par le moteur de recherche éponyme grâce à l'acquisition en 2004 de la société de cartographie numérique Keyhole. L'internaute peut « survoler virtuellement », à partir de photographies satellite, le Grand Canyon, la ville de Londres, la baie d'Osaka, des sites militaires ou quelques centrales nucléaires. Même si les informations ne sont pas diffusées en temps réel, la technique mise à disposition de *tous*¹⁴ découvre une nouvelle forme – *individualisée* – de « panoptisme planisphérique », libre de se « déplacer » et de zoomer « au-dessus » de l'ensemble de la Terre.

Cette faculté induit un accès ouvert à des images sensibles, pouvant faire l'objet d'une utilisation en vue d'actes illicites, notamment terroristes, qui témoigne de l'extension de nos capacités à visualiser les différentes « surfaces » de nos réalités, suivant des procédés et des proportions qui ne correspondent plus à l'échelle du corps. Quantité de nouvelles *prothèses* découvrent des panoramas d'observation, non seulement opérés à distance (la vidéosurveillance, par exemple), mais toujours plus éloignés du modèle anthropomorphique, celui qui envisage la technique comme un *substitut* compensatoire et élargi de nos contraintes physiques. Cette démesure, qui ne correspond pas à une *hybris*, plutôt à une sorte de « hors-mesure », structure les technologies du XXI^e siècle, définitivement à l'écart de la fonctionnalité historique envisagée comme un *prolongement* du corps, sur lequel se sont fondées les analyses de la *technè*, de Platon à Rousseau et à Heidegger. Une large partie de la technoscience de notre temps ne se détermine plus en fonction de la figure anatomique en vue d'augmenter ses capacités physiologiquement limitées de production ou de transport, mais vise désormais l'*implémentation* universelle de protocoles électroniques de *signal*, appelés à capter ou à émettre des *fréquences*, selon un ensemble de dispositifs toujours plus *intégrés* et *interopérables*, destinés au *suivi* et à l'*interprétation* ininterrompus des individus (de leurs tracés, de leurs désirs d'achats, de leurs intentions délictueuses, du fonctionnement de leur organisme...).

Récents virtualités permises par la convergence de l'*interconnexion*, de la *géolocalisation*, de l'extension exponentielle de *bases de données*, et de l'introduction de *puces* dans les tissus humains (à l'avenir selon des proportions *nanotechnologiques*). Dimensions qui tendent vers une sorte de « point Oméga », non pas celui défini par Teilhard de Chardin comme un moment dans l'histoire qui verrait la réalisation d'un ensemble parfaitement commun et homogène, mais comme la *réalité*, celle-ci advenue, d'une capacité de développer des procédures de surveillance et d'*alerte* selon une portée *globale* – qui brise avec évidence et frayeur toute conception linéaire de l'histoire en général ou de celle particulière, mais décisive, des techniques.

« Voir est un acte divin », disait Ludwig Feuerbach ; l'immémoriale quête humaine à vouloir se rapprocher de Dieu (ou du Ciel) a probablement trouvé dans l'*omnipotence satellitaire* une de ses formes *parfaitement* achevées et automatisées. « L'écran-monde du moteur de recherche de Google Earth se substituant tout à fait à l'horizon des apparences phénoménologiques¹⁵. »

1- Ce fut le premier conflit de l'*interconnexion* et de la *géolocalisation* généralisées, entendues comme des moyens décisifs capables d'assurer la suprématie militaire (toutes les unités étaient à la fois connectées à un centre de commandement et situées en temps réel sur des cartes grâce au système GPS).

2- Suivant le nouveau concept de « Revolution in Military Affairs » (RMA).

3- « Today's War Room is not only in a position of being able to access its branches'databases, but it can also draw on information from all over the world, from newsrooms, satellite image providers, libraries, etc. But also from databases in various information services, or secret and surveillance services, which cannot be entered either by public or commercial access rights » (Krystian Woznicki, « Beyond the Event Horizon. The War Room as a Mass Media System », in 5 *Codes, Architecture, Paranoia and Risk in Times of Terror*, Birkhäuser, 2006, p. 264).

4- « La nouvelle politique, surnommée « aplanissement du terrain » par l'administration Clinton, implique des arrangements pour le collectage, la réception et l'utilisation de renseignements secrets au bénéfice du commerce américain » (Duncan Campbell, *Surveillance électronique planétaire*, Allia, 2001, p. 91).

5- Traduction Pascal Delamaire, cf. <http://hypo.ge.ch/www/cliotexte/html/discours.eisenhower.html>.

6- Seymour Melman, professeur à Columbia University, New York ; cf. un entretien intitulé « On the Conversion Project », in Bruce Mau, *Massive Changes*, Phaidon, 2004, p. 174-175.

7- Un rapport daté d'octobre 2005, intitulé « Guerre et paix au XXI^e siècle » et rédigé par le Human Security Center de l'université de Colombie-Britannique, révèle une réduction chiffrée du nombre de guerres, de génocides et de violations des droits de l'homme depuis 1992.

8- Cf. le rapport de prospective géostratégique du département de la Défense, publié en février 2008.

9- Sur ces questions, cf. Michel de Certeau, *L'Invention du quotidien. Arts de faire, op. cit.*

10- Le « Panopticon » de Jeremy Bentham reste circonscrit à un cadre spatial *clos* et spécifique.

11- Sze Tsung Leong, « Espace-contrôle », in *Mutations*, Actar, Arc-en-rêve, 2000, p. 187.

12- Winston Churchill affirmait au début de la Seconde Guerre mondiale : « Nous sommes entrés dans l'âge des conséquences. »

13- Lettre à Mlle Leroyer de Chantepie, 6 juin 1857.

14- D'autres sites proposent le service : World Wind (mis au point par la NASA, selon un système « *open source* »), TerraServer, ou plus récemment l'offre de Microsoft : MSN Virtual Earth.

15- Paul Virilio, *L'Université du désastre*, Galilée, 2007, p. 31.

III

VIDÉOSURVEILLANCE

Anticipation « précognitive »

Quadrillage universel et exponentiel

D'abord analogique puis numérique, la vidéosurveillance représente la technique majeure qui a devancé depuis une trentaine d'années les écoutes téléphoniques en termes de volume d'utilisation, également d'un point de vue symbolique, par le fait de sa puissance sournoise supposée être toujours potentiellement en action. Quantité de procédés au cours de l'histoire ont cherché à développer une sorte de formule idéale, fondée sur la capacité d'observer à distance sans être vu. La *télé*-surveillance offre cette dimension d'ubiquité rêvée, suivant une extrême légèreté des dispositifs et une économie substantielle en moyens humains. Une technologie capable de fournir des images sans nécessiter une présence physique constitue une sorte de protocole parfait, qui a « naturellement » connu depuis son avènement une expansion sans cesse croissante. Dans *Le Cercle rouge* de Jean-Pierre Melville, Yves Montand opère un repérage à l'intérieur d'une bijouterie place Vendôme, et dit ensuite à ses complices : « Il y a des caméras de télévision partout. » Le film date de 1970 et signale en filigrane l'amorce d'un phénomène, autant que l'absence d'un terme lexical encore fixé. Il s'est opéré depuis le milieu des années soixante-dix une « infiltration » continue et progressive de circuits vidéo à l'intérieur d'une infinité d'espaces publics et privés : trottoirs et axes de circulation, parkings, gares, aéroports, centres commerciaux, entreprises, universités, écoles, stades, métro, bus, cimetières... Une telle densité suppose que la course de chaque individu est susceptible de pénétrer dans un champ de vision virtuellement omniprésent, théoriquement capable de suivre à la trace une « cible » humaine dans nombre de ses mouvements.

La vidéosurveillance a profité de plusieurs facteurs concomitants et favorables à son expansion. Elle a d'abord été envisagée comme une parade supposée efficace apte à inverser une augmentation statistique – presque continue depuis une trentaine d'années – des délinquances et incivilités commises dans l'espace urbain. Elle s'est développée simultanément à une

prolifération de discours politiques exposant la « sécurité » des citoyens comme un impératif prioritaire, suivant des orientations généralement démagogiques, bien plus rarement comme le résultat de réflexions relatives aux justes outils et dispositifs à mettre en place, en vue de répondre au mieux à ces objectifs, à l'intérieur d'un cadre démocratique fondé sur le respect des droits et devoirs de chacun. La menace terroriste croissante a rendu politiquement légitime son expansion. La diminution des coûts induite par la taille du marché ainsi que par le passage au numérique a contribué à ce qu'elle soit perçue – notamment par les municipalités – comme une solution somme toute avantageuse au sein de l'équation élémentaire qui évalue le rapport avantages/inconvénients. Elle a encore été envisagée comme un mécanisme qui revêt plusieurs atouts, prioritairement celui d'offrir une sorte de panoptisme « soft », capable d'observer à distance et en continu, sans effet de présence massive jugée agressive. La légèreté et la discrétion des systèmes ont concouru à entretenir cette dimension, autant qu'à faciliter leur extension.

L'inquiétante tension entre visibilité et invisibilité des caméras favorise un climat de « virtualité », ici entendue comme une possibilité sans cesse potentiellement à l'œuvre, qui instaure un rapport à l'espace public et privé sous la forme d'une *intériorisation* socialement inscrite du suivi ininterrompu des corps par des viseurs. Cette éventualité inlassablement en puissance de l'enregistrement de sa propre image correspond au pouvoir dégagé par le *Panopticon* de Bentham dont les effets ont été minutieusement décrits par Michel Foucault, particulièrement celui d'un « surmoi » disciplinaire omniprésent : « L'effet majeur du Panoptique : induire chez le détenu un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. Faire que la surveillance soit permanente dans ses effets, même si elle est discontinuée dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice ; que cet appareil architectural soit une machine à créer et à soutenir un rapport de pouvoir indépendant de celui qui l'exerce ; bref que les détenus soient pris dans une situation de pouvoir dont ils sont eux-mêmes les porteurs¹. »

Notre histoire occidentale, imprimée par les Lumières, a perçu l'individu prioritairement comme un être de raison, et a situé ses « passions » comme étant à l'extérieur de lui-même, résultats de « débordements » accidentels, excités par des effets d'ignorance ou d'irrationalité. Ces déficiences appellent certes des lois et une police, mais l'impératif social et éthique de la modernité fut d'abord celui de l'éducation et du travail. C'est sur ce fond épistémologique et culturel que se fonde notre perception de la juste tension entre, d'une part, la conception d'un citoyen libre et responsable, et d'autre part la nécessité de protéger son intégrité à l'encontre de personnes malveillantes ou « hors la loi », l'exigence de sa protection venant symboliquement en second, avant celle de son épanouissement comme être rationnel, selon une construction qui hiérarchise les priorités sociales, sur une

sorte de « déconnexion », voire une antinomie, entre autonomie et sécurité. Pour aller vite (nous y reviendrons), la récente opposition entre Europe et États-Unis s'établit, pour la première, sur la volonté de maintenir cet ordre historique, et, pour les seconds, sur celle de l'*inverser* en vue de faire jouer autrement cette relation, selon une conception du droit et de l'ordre qui ébranle certaines dimensions éthiques et juridiques fondatrices des démocraties modernes.

Paradoxalement et contrairement à quantité d'idées reçues, le succès de la vidéosurveillance, notamment favorisé par de nombreux responsables politiques, serait dû au sentiment de préserver cet ordonnancement : une présence discrète, seulement dressée en vue de prévenir ou de constater des infractions, l'intention supposée étant seulement de protéger sans pouvoir *intrusif*. Les cadres juridiques qui bornent son utilisation exigent une *pertinence de l'usage* (surveillance des espaces publics, des réseaux de transport...), et interdisent généralement un archivage au-delà d'une durée de trente jours. Rien ici qui imposerait un « renversement des valeurs ». Néanmoins, ce qui pourrait à terme induire une bascule historique ne se restreint pas au seul fait de la vidéosurveillance, mais à ses nouvelles *capacités d'analyse* des images et des comportements reliées à des *bases de données*, susceptibles d'étendre selon de toutes autres mesures spatiales et temporelles la « profondeur de champ » dans la captation des individus, selon une formule bien distincte de celle d'un simple « cadrage » momentané et occasionnel.

Le 7 juillet 2005, une série d'attentats frappe Londres. La ville représente – avec Manhattan – le territoire le plus « quadrillé » de la planète. La densité des systèmes de vidéosurveillance est, au Royaume-Uni, la plus élevée au monde. On estime que chaque citoyen britannique serait filmé, selon différents « angles », à trois cents reprises quotidiennement. Cette couverture quasi globale a permis aux policiers britanniques de visionner plus de trente-cinq mille bandes et fichiers à la suite de ces événements. Les images de centaines de milliers de visages ont été scrutées au sein de masses compactes, parmi lesquelles il a pu être dégagé celle de Hasib Hussain, traversant le 7 juillet 2005, à 7 h 20, la gare de Luton, équipé d'un sac à dos censé contenir les explosifs qui ont tué quatorze personnes dans un autobus à Tavistock Square. Le 21 juillet, à 12 h 36, Mokhtar Saïd Ibrahim a été filmé par la caméra embarquée dans un bus à impériale, à l'étage duquel il est soupçonné d'avoir tenté, sans succès, de faire exploser sa bombe. Les enquêteurs ont pu reconstituer les itinéraires grâce aux documents vidéo ; dès le 12 juillet, ils savaient que les quatre auteurs de la première vague d'attentats étaient arrivés en train au centre de Londres et s'étaient retrouvés à la gare de King's Cross, vingt minutes avant les explosions. Le 22 juillet, soit le lendemain des attentats manqués, Scotland Yard diffusait des images des quatre terroristes présumés. Parallèlement, la police invitait la population à transmettre toute

information jugée utile, suivant un usage à l'œuvre dans le cadre d'investigations criminelles, qui a encore contribué à l'efficacité et à la réussite de l'enquête.

Les polices du monde entier furent impressionnées par la qualité des résultats obtenus grâce à une méthode dont l'outil principal consistait à envelopper la ville de viseurs enregistreurs, et à envisager les images comme *révélatrices* d'indices décisifs, orientant l'ensemble des recherches. De nombreux services de sécurité français et étrangers ont depuis avancé qu'« il y aura peut-être un avant et un après Londres », relativement aux moyens technologiques déployés par leurs collègues britanniques pour traquer et identifier les poseurs de bombes des 7 et 21 juillet 2005. Le 11 septembre 2001 a marqué une rupture historique à l'égard de la relation que certains États, et particulièrement les États-Unis, pouvaient entretenir au *renseignement*, envisagé depuis comme le *socle* stratégique déterminant, seul capable de cartographier les risques et de les *prévenir*. L'opposition à l'égard de la « nébuleuse terroriste » impose une architecture de défense dont la captation d'informations constitue le fondement cardinal, première articulation décisive, apte à *signaler* la nature et le volume des attaques en préparation. C'est conformément à cette logique que s'est formé en quelques années (simultanément à une sophistication continue des technologies) un environnement planétaire *pénétré* d'instruments de collecte de données toujours plus *sensibles* et *densifiés*.

Les attentats de Londres de juillet 2005 constituent un autre type de rupture relativement à la façon dont les organes de sécurité (ministères de l'Intérieur, polices, agences de renseignement) perçoivent désormais la vidéosurveillance. Jamais dans l'histoire moderne de la police judiciaire, le recours aux enregistrements des caméras, allié aux techniques d'investigation traditionnelles, n'a été revendiqué à une aussi grande échelle pour traquer des criminels présumés. L'étendue de la « couverture » à Londres, qui a rendu possible une investigation *a posteriori* extrêmement efficace, impose dans les faits l'outil comme un dispositif décisif non pas tant en termes de dissuasion qu'en termes d'instrument d'enquête indispensable et nécessaire à un arsenal complexe, destiné, sous diverses formes, à s'opposer aux forces dissimulées du terrorisme. Une nouvelle légitimité a été acquise depuis ces événements, qui a encouragé au-delà de toute mesure précédente une utilisation étendue – particulièrement en Europe, jusque-là plutôt réticente à une généralisation de la vidéosurveillance. Depuis, le taux d'assentiment en Grande-Bretagne relatif à ces mesures, estimé au cours de sondages successifs, se situe aux alentours de 70 %, suivant des perceptions rapidement considérées comme quasi unanimement approuvées, associant *de facto* vidéosurveillance et sécurité, favorisant consciemment et inconsciemment une infiltration continue d'yeux électroniques dans l'environnement. Cette omniprésence a encouragé Manu Luksch, artiste autrichienne installée à Londres, à réaliser un film intitulé

Faceless, composé exclusivement d'images de vidéosurveillance : « Un projet rendu possible grâce à la loi britannique sur la protection des données qui permet aux personnes filmées de réclamer une copie des enregistrements où elles apparaissent. Il y avait tellement de caméras partout que j'ai trouvé superflu de rajouter la mienne². »

Suite aux attentats de Londres, plusieurs gouvernements européens ont décidé de modifier leur législation afin de faciliter l'utilisation de circuits vidéo. Le Parlement français a voté en décembre 2005 une loi « antiterroriste » en partie inspirée de l'exemple britannique. Le premier chapitre du texte stipule qu'elle a « pour objet de permettre un développement du recours à la vidéosurveillance afin d'accroître la protection des principaux lieux accueillant du public et des installations exposées à une menace d'acte de terrorisme ». La loi autorise un emploi plus systématique et plus étendu de caméras, aussi bien par les organismes d'État que par des personnes morales de droit privé, en vue de protéger certains types de bâtiments (lieux de culte, compagnies aériennes, entreprises « sensibles »). L'incertitude de la menace appelle presque « naturellement » un réflexe sécuritaire, dont on espère – par pure hypothèse et sans garantie aucune – que la technologie pourra autant que possible prémunir de certains dangers. Cette tension irrésolue entre « abstraction » et réalité de la menace, ne pouvant se dénouer une fois pour toutes, induit des comportements de nature impulsive qui concourent à un élargissement du cadre d'usage et juridique de la vidéosurveillance. Et ce, simultanément à un entrelacement de plusieurs techniques et de facteurs hétérogènes, qui participe de ce « bouillon de culture » évoqué plus haut et instaure un environnement sans cesse plus *infiltré* par des dispositifs automatisés de suivi des corps et des comportements.

« *Précognition* »

On peut juger le nouvel impératif d'*anticipation* (s'efforcer de *devancer* la menace par un « scannage » universel de tous les individus) contraire à certains droits fondamentaux, notamment celui de la « présomption d'innocence », non pas entendue ici dans sa signification juridique usuelle mais dans un cadre social plus élargi qui devrait s'interdire d'envisager systématiquement – sous forme de vérifications continues – chaque citoyen comme étant en permanence un coupable potentiel. La captation « sans rupture » opérée par les technologies numériques, particulièrement la vidéosurveillance, produit un renversement du rapport entre intention et acte. La force policière n'est plus envisagée comme devant dissuader par sa présence ou collecter des indices *suite* à des délits produits, mais comme devant *collecter* des données *avant* la réalisation d'une action, sous la forme exacte d'un *retournement* de sa fonction dans l'ordre social, non plus dressée en vue de veiller à *distance* au respect des lois mais de se rapprocher *au plus près des corps* en vue de leur constante « dissection ».

Le personnage de Tom Cruise, dans *Minority Report* (film de Steven Spielberg, réalisé d'après le roman éponyme de Philip K. Dick), est responsable d'un programme de sécurité fondé sur une *prémonition* des actes rendue possible grâce à des créatures, les « precogs », dotées d'un don de « précognition » – capacité de perception extrasensorielle –, qui signalent toute velléité meurtrière et déclenchent l'envoi d'une brigade d'intervention *antérieurement* à la réalisation d'un délit. Entrelacements d'organes corporels et numériques permettent de maintenir un taux zéro de criminalité. D'une certaine façon, les protocoles automatisés de surveillance contemporains, leurs capacités de *veille*, d'*analyse* et d'*alerte*, légitiment le fantasme d'un ordre établi sur la capacité à recueillir *en amont* les informations nécessaires, en vue de devancer les méfaits et de s'opposer à leur exécution. De la même façon que durant la première guerre du Golfe (1991), le concept de « guerre propre » est apparu sous la forme d'un véritable oxymore ; celui de « dispositif sécuritaire anticipatoire » pourrait désigner et catégoriser la propension à instaurer la *quête informationnelle* comme l'objectif pivot d'une nouvelle lutte de nature *préventive* contre *toutes* les insécurités. Cette ambition de « précognition » impose un nouveau paradigme, fondé non plus sur le jugement juridique qui évalue *après coup* l'acte commis en fonction des lois en vigueur, mais sur un examen généralisé *a priori*, situant *de facto* le rapport fondamental de chaque individu à la collectivité sur fond structurel de *suspicion*.

Un des grands acquis philosophiques et éthiques de la postmodernité a consisté en une réhabilitation (d'esprit aristotélien) de l'*expérience singulière* au détriment d'universaux ignorants la spécificité de chaque situation propre. Contre des impératifs abstraits et figés, pour la plupart issus de l'universalité des Lumières, une morale – organique – du *cas par cas*, capable d'évaluer les actions dans un large contexte (psychologique, social, économique) s'est peu à peu étendue depuis le milieu des années soixante-dix, notamment par le fait de certaines analyses de la philosophie française (particulièrement Jean-François Lyotard, ou l'*Éthique du contrat* de Paul Ricœur). Dans le même mouvement, une très large part de la socialité s'est développée suivant ces principes de particularité des *cas de figure* (perception croissante de l'individu comme « unité d'exception » qui induit quantité d'incidences ; citons-en certaines : suivi de *chaque* parcours professionnel et encouragement à la formation continue opposée à la fixité des qualifications ; traitements médicaux toujours plus *personnalisés* ; *individualisation* des offres commerciales – contre les « segments » de population, maintenant jugés trop vagues –, notamment à l'œuvre dans le marketing, si alerte à exploiter des données philosophiques et anthropologiques). Notre *épistémé* contemporaine est caractérisée par le privilège désormais accordé à l'*expérience singulière* au détriment de classifications nébuleuses et rigides. Les « multi-appartenances » identifiées par François Ascher³ signalent les effets de *mobilité* et d'*originalité* propres à chaque existence.

L'ensemble de cet environnement culturel désormais fondé sur la *priorité* octroyée à l'unité individuelle et mouvante, au détriment de la masse impersonnelle et compacte, pourrait à nouveau être renversé par la *réduction* de toute personne à une commune « logique du soupçon », indifférente à l'épaisseur insolite de chaque conjoncture. Il se dessine depuis peu une nouvelle distinction entre, d'un côté, ceux qui estiment pouvoir et devoir évaluer *a priori* un acte, et d'un autre côté ceux qui jugent qu'un acte ne peut être évalué qu'*a posteriori* ; opposition qui marque une divergence de conception fondamentale à l'égard de ce qui structure le tissu social. Une récente position politico-juridique (formulée au début de la première décennie du XXI^e siècle par les « néoconservateurs américains », mais reprise plus largement sur de nombreux territoires) s'inquiète d'un nouveau type de rapport dangereusement *asymétrique* à la loi (la grande majorité y répond, mais une infime minorité, disposée à commettre des actes de « terreur », est susceptible de mettre en péril la société). Situation qui oblige – vu l'ampleur des risques, particulièrement celui probablement à venir du terrorisme bactériologique ou nucléaire – à se saisir de toutes les armes à disposition, dont la plus puissante est l'infiltration *tous azimuts*, destinée à décrypter en amont la préparation d'une opération (disposition qui a tant fait défaut lors des événements du 11 septembre 2001).

La position démocratique historique suppose, elle, la *logique du contrat*, envisagée comme un pacte partagé qui intègre la possibilité de la faute ou du conflit (arbitré par des instances de jugement *a posteriori*, tribunaux de toute sorte), mais sur fond de responsabilité individuelle garantie par la majorité légale et la raison (ce pourquoi les « déficients mentaux » ne peuvent être jugés). Cette posture admet l'hypothèse du crime (comme un phénomène social limité, grâce à la rationalité des citoyens) ; l'autre ne peut l'accepter (au vu des conséquences désastreuses éventuelles, et au nom d'une tout autre conception de la socialité, non plus fondée sur un *pacte de raison* mais perçue comme un champ toujours miné qui oblige inlassablement à déminer, à *vérifier* sans fin l'état du terrain, dans une société prioritairement et globalement déterminée par la *virtualité omniprésente de la catastrophe*). Si cette propension tend à se légitimer par l'incertitude du péril terroriste, elle « infiltre » sournoisement, selon les mêmes logiques, d'autres dimensions du quotidien : établissements scolaires, lieux de travail, jardins publics..., placés sous vidéosurveillance, selon des visées hybrides (enregistrement indifférencié en vue de recueillir d'éventuelles traces ou de produire un effet dissuasif, ou encore de soumettre des zones à des protocoles de « veille continue » capables d'*alerter* au moindre danger ; disposition excitée par une sorte d'inconscient collectif qui voudrait inscrire la force policière comme un pouvoir de *réactivité* humain et technique, coordonné par une nouvelle aptitude systématisée et automatisée de « précognition »). Il est possible d'affirmer ici, sans aucune velléité futurologique, que le programme de

sécurité à l'œuvre dans *Minority Report* représente *tendanciellement* et *structurellement* l'avenir du rapport entre individu et loi, toujours plus interféré par des instances (équipes et technologies robotisées) de surveillance aptes à se déployer grâce à une couverture toujours plus globale et suivant des vitesses « sans délai », dont la perfection correspondrait au fantasme de la quasi-simultanéité : le *temps réel*, ou mieux encore : le coup d'avance ou *un temps avant*.

Deux facteurs décisifs concourent à instaurer cette *matrice* du XXI^e siècle : menace terroriste et puissance du calcul électronique, qui poussent *ensemble* vers une forme de « scannage ininterrompu du corps et de ses actes ». Également des *désirs*, dans la mesure où le marketing contemporain fonde son socle stratégique sur l'analyse et l'*anticipation* suivies des comportements individuels, comme un signe patent de l'expansion continue de la matrice : son *infiltration* à l'intérieur de quantité de champs hétérogènes composant notre *quotidien*. Un nouveau milieu se forme, se développe, s'étend, dont la portée des incidences ne se restreint pas à quelques secteurs identifiés et délimités, à tel point qu'il modifie plus largement et en profondeur la notion anthropologique de *rapport de force*. Dimension aujourd'hui trop souvent ignorée, au profit de perceptions naïves et de bons sentiments qui occultent la force du *différend* entre chaque entité, historiquement entendu comme jeu d'opposition capable de se contredire ou de réaliser finalement des *compromis*. Désormais, ce principe se déploie à l'intérieur d'une grille au sein de laquelle la *profondeur de pénétration* prévaut, qui repousse lutte et conflit (concepts des XIX^e et XX^e siècles), au profit d'un nouveau type de *pouvoir anonyme* institué sur un don de *transparence*. Double transparence : du côté d'une *invisibilité* croissante des dispositifs – *intégrés* ou « *immatériels* » –, et du côté d'une *dissection* de chaque individu, selon une acuité clinique. La nature du tissu relationnel (entre personnes, groupements, instances politiques, économiques...) est reconfigurée et le sera sans cesse davantage par cette nouvelle *asymétrie* sans précédent historique – entre organismes de toutes sortes et citoyens –, qui ne peut être véritablement contredite par aucune stratégie de type dialectique (manifestations, associations, forums...), trop faible à l'égard de processus qui prolifèrent selon des schémas organiques et *discrets* que rien ne peut massivement interrompre, mais qui sont aptes à être *modulés* par une vigilance individuelle et collective soutenue, associée à la force concertée de la *loi*.

Cependant, la dimension légale telle qu'elle se rédige actuellement ne suppose pas nécessairement au cours de cette première décennie du XXI^e siècle – décisive relativement aux « enjeux sécuritaires », dans la mesure où les situations ne sont pas encore précisément « fixées », mais en *gestation* provisoire – une récusation systématique de ces logiques, mais contribue parfois à les accompagner, à les amplifier, à les ancrer même dans l'environnement (les lois Patriot Act I & II, sur lesquelles nous reviendrons,

sont emblématiques de l'intériorisation et de l'aménagement social systématique de l'ambition de *transparence*). D'une certaine façon, l'opposition récente entre États-Unis et Europe se fonde notamment sur une différence de perception relativement à la *fonction* de la loi. Du côté américain, elle est envisagée comme une *arme* – reconnue et admise – en vue de lutter contre l'incertitude terroriste prioritairement par la puissance technologique de « pénétration intrusive » ; du côté européen, la loi est généralement considérée comme une *protection* indispensable à l'égard des instances de sécurité, naturellement enclines à radicaliser les protocoles d'observation au nom de leur mission, ce pourquoi en Europe toute loi qui renforce les pouvoirs de sécurité est d'abord perçue comme liberticide.

Il est possible de renvoyer dos à dos les deux conceptions et d'affirmer que la valeur de la loi ne consiste ni à positionner chaque individu comme une cible scannée en continu, ni à l'entendre comme un « contre-pouvoir » suivant un angélisme qui oppose sécurité à liberté, mais comme un « régime » propre dont la valeur ne peut se réduire à une instrumentalisation brute mais doit se construire dans un écart, celui qui permet d'examiner à distance la complexité des enjeux et de tracer certaines limites jugées primordiales à l'égard de l'intégrité de chacun et de l'exigence démocratique. Néanmoins, la dimension généralement nationale des lois relatives aux enjeux sécuritaires – alors que leurs champs d'application relèvent toujours davantage de dimensions transnationales – impose *de facto* des différences qui traceront une cartographie planétaire très contrastée ; sources de conflits dans la mesure où la captation des données ignore en grande partie les frontières politiques. Idéalement, une borne infranchissable et jugée universelle devrait proscrire aux instances publiques ou privées de disposer d'« *armes de transparence totale* », dont la forme déjà identifiée et jusque-là encore illégale se nomme « *agrégation globale de données* », qui ambitionne de *croiser* les sources *éparses* et de dresser en temps réel des profils « intégraux » en fonction d'informations extrêmement hétérogènes (achats, transactions bancaires, déplacements, dossier médical, appels téléphoniques, navigation Internet...).

Une forme de paradoxe se développe : l'objectif de garantir la sécurité des personnes appelle *en retour* un effort d'« auscultation » de chacun suivant un « *double bind* » (une « double contrainte » selon les théories de la communication, entendue comme une impossibilité de choisir entre deux registres distincts), qui caractérise en partie la structure extrêmement nouée qui forme ce balancier instable, qui perturbe ou inverse des modèles éthiques, sociaux et juridiques pour la plupart à l'œuvre depuis les Lumières, établis sur un équilibre constamment recherché entre liberté absolue des êtres et sauvegarde de l'État. Alors qu'historiquement la surveillance généralisée des populations relevait davantage du fait d'oligarchies ou de dictatures en vue de maintenir des assises vulnérables, ce sont aujourd'hui les démocraties, à l'intérieur d'une période angoissée par la nébuleuse terroriste, qui se

rapprochent de ces schémas panoptiques, alors que l'intention déclarée initiale vise la protection des citoyens. Ici doit être pointée la caractéristique spécifique des appareils numériques : machines de captation, d'analyse et d'alerte qui favorisent des modalités d'usage à ce point « virtuelles » qu'elles « s'auto-accroissent d'après leurs propres logiques », selon les termes de Jacques Ellul⁴, qu'elles *devancent* sans fin la loi et découvrent des pratiques frappées par des vides juridiques que le législateur doit sans cesse, et dans un second temps, s'efforcer de combler.

Nous sommes confrontés à un double jeu entrelacé des *effets*, d'abord celui de la volonté politique d'être irréprochable dans la gestion de la menace terroriste, et qui pour cela peut être appelée à radicaliser ses décisions, ensuite celui des dispositifs techniques contemporains offrant des capacités expansives de « scannage » et de pénétration de l'*intégrité individuelle*. Il apparaît un horizon marqué par une *instabilité* continue qui suscite une pathologie de la *protection*, sournoisement et progressivement devenue la *priorité* sociale et géopolitique. Nous évoluons désormais à l'intérieur d'une période qui découvre un enjeu majeur, celui qui consistera à devoir gérer, dans l'*incertitude*, l'équation fragile qui mêle *risques terroristes / développements techniques / cadres juridiques*, suivant un triangle dont le maintien du juste équilibre ne repose pas sur des solutions déjà enregistrées mais qui requiert des solutions inédites et viables, nécessairement soumises au jeu informé et concerté de la *délibération*, à l'intérieur de cadres autant nationaux que transnationaux.

Certaines perceptions de la valeur de la vidéosurveillance contribuent à opérer de nouvelles *torsions* sur cette figure triangulaire extrêmement plastique, notamment celles qui l'envisagent comme un moyen efficace de « prévention situationnelle », supposé rendre quasiment impossible l'exécution d'infractions. Postulat qui présume l'œil de la caméra doté d'une même puissance de dissuasion qu'une présence policière, par exemple. Comme il est impensable et absurde d'imaginer des forces de l'ordre déployées en continu dans les espaces publics ou privés, alors apparaît l'hypothèse d'une « couverture globale » par les circuits vidéo ; nouveau palliatif discret et toujours en veille, apte à semer une frayeur consciente et inconsciente contre l'exécution d'un délit. On peut critiquer le réductionnisme naïf de cette approche qui occulte la part des facteurs personnels, familiaux et sociaux susceptibles de conduire à la délinquance. Cet axiome s'appuie non seulement sur des fondements erronés, mais il contribue davantage à opérer une tension inédite au sein du triangle évoqué, envisageant l'*infrastructure technique* comme l'armature de protection pivot qui devrait être suivie par la loi et les budgets de dépense publique. Le principe de « prévention situationnelle » induit le déploiement d'un environnement au sein duquel l'effort en vue d'*empêcher* des forfaits constitue la *strate conditionnelle* à toute entente communautaire.

En tout état de cause et quelle que soit sa légitimité, un tel positionnement devrait au moins être en mesure d'argumenter en fonction de preuves valides : des statistiques de terrain. (11/09/01, 5 h 45, Mohammed Al-Amir Atta et Abdulaziz Alomari sont filmés à Portland [Maine] avant d'embarquer dans une navette qui les déposera à l'aéroport de Boston. Les deux terroristes prendront ensuite le premier des vols qui s'écraseront contre le World Trade Center.) De nombreux travaux de recherche (dont plusieurs menés en Grande-Bretagne) établissent que la vidéosurveillance occasionnerait des effets extrêmement limités sur le volume de la criminalité et qu'elle favoriserait en retour un déplacement vers d'autres quartiers moins surveillés. Peu de chiffres sont disponibles pour confirmer ou non son efficacité. À l'écart du fantasme naïf de la *prévention situationnelle*, doit être relevé le fait que l'expansion continue d'yeux électroniques dans les espaces urbains contribue insidieusement à développer une forme d'*intérieurisation* de formes permanentes de surveillance dans les consciences, et ce, que les dispositifs soient visibles ou non, efficaces ou non, à l'intérieur d'une nouvelle matrice sociale qui, à défaut d'être déjà capable d'analyser jour et nuit les déplacements et actes quotidiens, pousse à coup sûr chacun à se représenter sans cesse vu, identifié, suivi à la trace, suivant des schémas troubles et incertains, situés entre réalité avérée et imaginaire inquiétant. À propos du *Panopticon*, Foucault signalait encore : « Il n'est pas nécessaire d'avoir recours à des moyens de force pour contraindre le condamné à la bonne conduite⁵. »

La veille électronique permanente produit parfois des effets inverses à ceux recherchés et permet d'établir des actes illégaux commis par des instances de sécurité (polices nationale ou municipale, vigiles), qui induit une sorte d'*horizontalisation* indifférenciée des cibles surveillées. Événements de plus en plus fréquents qui défont certains clichés binaires au profit de schémas qui rendent visible le glissement du statut des uns et des autres. La généralisation des téléphones portables munis de caméras a encore encouragé certaines personnes à saisir des images d'exactions et abus perpétrés par des unités militaires (issues particulièrement des armées américaine et britannique en Irak). Documents à charge souvent pris à la sauvette – rendus réalisables par le fait de l'expansion des dispositifs individuels *miniaturisés*, qui contribuent à intensifier la grille universelle de vidéosurveillance – et aussitôt diffusés en « quasi-temps réel » sur les écrans de la planète ou les sites de « partage vidéo ».

L'implantation de circuits ne s'opère plus seulement sur des lieux fixes mais également à l'intérieur de surfaces *mobiles*, davantage disposées à appréhender des cadences de flux instables (véhicules espions, par exemple), ou encore à « encadrer » des événements « nomades ». Une société française, la Sofema, a conçu le principe d'un ballon dirigeable gonflé à l'hélium, équipé d'yeux électroniques. Les caméras embarquées permettent de zoomer

sur un visage ou de percevoir une plaque d'immatriculation à plus de cinq cents mètres d'altitude. Le dispositif est maintenant régulièrement utilisé en vue de la surveillance maritime, du trafic routier, ou à l'occasion de « rave parties » et de manifestations. La matrice universelle de surveillance se *densifie* par l'investissement de cette strate située entre sol et satellites extra-atmosphériques, suivant des fonctionnalités distinctes, aptes à gagner au fur et à mesure certains points de perception encore laissés vacants. À l'instar des avions radars américains « Awacs », jusque-là exploités à des fins militaires et désormais opérationnels – depuis le 11 septembre 2001 – dans le cadre d'événements à dimension planétaire : Jeux olympiques, Coupes du monde de football..., destinés à sécuriser l'espace aérien et à prévenir l'intrusion d'appareils détournés ou munis de charges menaçantes. C'est encore un autre « palier » du « Panopticon » contemporain qui ici se constitue et se consolide jour après jour, formé de structures technologiques multiples, qui, d'une certaine façon, s'*emboîtent* toujours davantage et se complètent, se « relaient » plutôt, suivant une trame universelle capable de dresser des *capteurs* configurés en fonction de *chaque* situation spatiale et cas de figure spécifique.

Il existe encore un autre plan – plus indéterminé – de surveillance, sous la forme d'une aggravation de sa dimension fantasmatique : l'installation d'objets recouvrant l'apparence exacte de caméras, cependant incapables de saisir la moindre image, seulement assignés à produire des effets supposés dissuasifs, sous l'aspect de *leurres*. Ces dispositifs, nombreux dans l'urbanité contemporaine, dans le métro parisien par exemple, visent non seulement à favoriser des phénomènes d'intimidation par jeux d'omniprésence, mais davantage à renforcer le principe d'une *intérieurisation* généralisée de la captation ininterrompue des individus, sans que le mécanisme soit véritablement à l'œuvre. Le seul fait de leur présence visible est d'abord envisagé comme un frein à toute velléité d'action illégale, mais induit plus encore une perception, partagée par le corps social, d'être dans son ensemble surveillé par des yeux dont on ne sait plus s'ils sont « voyants » ou « non voyants », ponctuant de point à point les espaces. Cette suspension incertaine, jamais résolue dans l'expérience quotidienne, contribue à établir dans l'inconscient collectif un rapport entretenu à l'environnement toujours plus marqué par une impression de *paranoïa*. Michel Foucault, à propos du *Panopticon* de Bentham, dégageait encore un type d'incidence produit par la ruse de son architecture, qu'on pourrait reprendre à la lettre à l'égard des conséquences causées par le *leurre* : « Il automatise et désindividualise le pouvoir. Celui-ci a son principe moins dans une personne que dans une certaine distribution concertée des corps, des surfaces, des lumières, des regards ; dans un appareillage dont les mécanismes internes produisent le rapport dans lequel les individus sont pris⁶. »

Les mailles de la matrice sont à ce point toujours plus resserrées qu'il

devient légitime de se demander s'il existe encore des « trous », quelques zones laissées vacantes au sein de notre « hypermodernité » ; dimension de saturation anticipée par Orwell : « Quelque chemin que l'on prit, on avait le télécran devant soi⁷. » La quasi-totalité des secteurs dits sensibles est déjà placée sous vidéosurveillance globale, à l'instar des grands aéroports internationaux. Le personnage principal du film de Steven Spielberg *Terminal*⁸ erre sans fin dans l'aéroport JFK, sans documents d'identité lui permettant de passer la douane, et incapable de retourner dans son pays d'origine par le fait d'un coup d'État soudain ; il se trouve balancé dans une situation suspendue qui lui octroie un statut aléatoire, l'obligeant à rester cantonné dans les immenses espaces clos de l'aérogare. La police de l'air suit ses parcours sur ses écrans de contrôle d'une façon continue, « sans rupture de plan », jusqu'à une séquence où, se trouvant juste en dessous d'une caméra dans un angle aveugle, son corps « sort du champ » malgré les multiples manipulations, rotations et zooms actionnés à distance par la cellule de sécurité. Cette scène pourrait être emblématique de notre environnement, caractérisé par une couverture à la fois sans cesse densifiée et ébréchée par une fragilité de fait, celle d'une impossibilité structurelle de mettre en place une réelle vidéosurveillance globale qui relève, doit-on le rappeler, d'une représentation chimérique. Cette crainte d'une vision panoptique pourrait en revanche se déployer très bientôt, non dans le cadre exclusif de la saisie d'images vidéo mais dans la réduction de chacun à des *codes* stockés, constamment actualisés en temps réel, d'après quantité d'actions hétérogènes commises, innervant les *bases de données* constituant dorénavant le *cœur* de l'architecture d'une nouvelle surveillance contemporaine toujours plus « omnisciente » – de surcroît *absolument invisible*.

Dans le film *The Recruit*⁹ (*La Recrue*), dans lequel Al Pacino joue le rôle d'un professeur de techniques de renseignement auprès de la CIA, on découvre lors d'une scène située dans un parking souterrain deux de ses étudiants qui voudraient s'embrasser alors qu'ils sont censés ne pas se fréquenter, et ne disposent que de vingt secondes avant que la caméra ne pivote à nouveau vers eux... ; autre signe patent de l'impossibilité de saisir la totalité des événements suivant une dimension sphérique et intégrale. *Look*¹⁰, film plus récent, met en scène cinq histoires parallèles dont les événements sont supposés être *exclusivement* captés par des circuits vidéo, exposant des vies singulières saisies en continu et à l'insu de tous les protagonistes. Entreprise dont on ne sait plus si elle constitue une sorte d'intensification radicalisée de la réalité ou sa simple représentation, cauchemardesque mais bien objective. Si l'on peut quotidiennement vérifier que se déploie au sein de lieux très fréquentés une couverture presque intégrale, comment comprendre que des zones plus ou moins dépeuplées soient également filmées en continu par des yeux électroniques ?

C'est l'objet d'une installation conçue par Thomas Köner, intitulée *Banlieue du vide*, dont les images proviennent d'une collecte de différents

paysages d'hiver que l'artiste a saisis sur Internet et dont il explicite les enjeux : « Ce sont trois mille prises de vue de caméras de surveillance. Les images choisies montrent des routes, filmées la nuit, désertes et couvertes de neige. La bande sonore se compose de parasites sonores [*grey noises*] et d'échos de la circulation provenant de ma mémoire. Le seul mouvement visible naît des amoncellements de neige couvrant les routes. » Cette œuvre, au contraire de nombreux travaux, notamment consultables sur la Toile, ne focalise pas l'attention sur la saturation des procédures de contrôle effectives dans l'urbanité contemporaine, mais insiste plutôt sur la *futilité* de certains dispositifs mis en place, au sujet desquels on peut naturellement être tenté d'évaluer leur pertinence relativement aux visées sécuritaires recherchées, manifestement inopérantes à l'intérieur de ces espaces presque abandonnés. C'est probablement une large part des circuits de vidéosurveillance qui pourrait être réévaluée à la mesure de cette *vanité*-là, circuits envisagés comme des mécanismes déployés pour nombre d'entre eux en pure perte, finalement incapables d'apaiser une fois pour toutes nos profondes angoisses, enclins à toujours vouloir *surprendre* davantage n'importe qui n'importe où, jusqu'aux écureuils traversant la nuit quelque champ dépeuplé et recouvert de neige...

La propagation de caméras engage d'une façon presque indissociable celle de salles de contrôle surchargées d'*écrans*, à l'instar de la société disciplinaire à l'œuvre dans le film de Terry Gilliam *Brazil*, gouvernée par une administration omnipotente dont tous les locaux sont systématiquement équipés de moniteurs à l'apparence désuète, ou encore dans *Minority Report*, dont les représentations « précognitives » sont d'abord visibles sur des *videowalls* translucides « hyper high-tech », aux interfaces faisant quasiment corps avec leurs utilisateurs. Plus largement, la prolifération ininterrompue de *surfaces écraniques* dans notre environnement constitue un phénomène technique, urbanistique et anthropologique majeur de notre période historique¹¹. Captation et manipulation d'informations sont sans cesse davantage médiatisées sous la forme de *pixels*, par le fait d'un usage quotidien de plus en plus massif d'écrans ; soit mobiles et miniaturisés (ordinateurs et téléphones portables, organiseurs, baladeurs MP3) ; soit toujours plus vastes et insérés à des façades architecturales (écrans géants) ; soit disposés dans les espaces publics, commerciaux ou domestiques, suivant des formes à la dimension d'*intégration* croissante (téléviseurs plasmas, bornes interactives, « murs-vidéo »).

Les cellules de visionnage sont généralement équipées de systèmes qui permettent aux agents de sécurité placés devant leurs écrans de zoomer sur les images, de lire une plaque minéralogique située à trois cents mètres du viseur, de déplacer les caméras à tourelle, et de prévenir à tout moment les brigades mobiles, suivant des délais d'intervention de plus en plus resserrés. Mais ces unités correspondent encore à des schémas qui nécessitent une présence

humaine, selon des configurations techniques déjà en voie de disparition au profit d'une *automatisation* digitale et robotisée des informations émises par la vidéosurveillance du XXI^e siècle. Non seulement le vocable de « cassettes vidéo » renvoie à un index obsolète, mais encore celui d'*image* subit un glissement vers une notion désormais plus pertinente : *données numériques* reliées à d'autres données, capables d'être traitées, analysées et *interprétées*, suivant un diagramme qui *superpose* quasi simultanément technologies de saisie des corps, d'évaluation de leur « degré de dangerosité », et d'*alerte* à des individus en « chair et en os » disposés au bout de la chaîne.

Vidéosurveillance « intelligente »

Les circuits vidéo sont appelés à être systématiquement reliés à différents types de logiciels capables de « comprendre » le contenu d'une image et d'alerter en fonction d'informations préalablement enregistrées. Certains d'entre eux, grâce aux recherches entreprises dans le cadre de l'« *analyse comportementale* » (*behaviour analysis*), sont configurés en vue de détecter des « postures suspectes ou déviantes », de saisir des gestes marqués par la nervosité, l'anxiété, ou encore des durées de présence à l'intérieur d'un même lieu jugées trop longues. Les principes qui déterminent ces classifications sont assurément perfectibles, et basés sur des expérimentations empiriques qui revêtent *de facto* des proportions d'erreur élevées. D'autres encore permettent de déceler des attitudes supposées contraires à une réglementation, par exemple un individu qui emprunterait un couloir de métro à contresens, un mouvement de foule inopiné aux abords d'un lieu sensible, un véhicule immobilisé sur une bande d'arrêt d'urgence d'autoroute... La reconnaissance de visages captés au hasard constitue une des fonctionnalités majeures offertes par la « vidéosurveillance intelligente », apte à comparer en temps réel les données avec les photos numériques stockées sur les fichiers de police ou ceux d'autres instances de sécurité.

La technique est utilisée par des casinos en vue de repérer les clients classés fragiles ou indésirables, ou par les aéroports internationaux pour identifier les traits de supposés terroristes déjà numérisés et archivés sur les bases de données, mais avec des « taux de rejet » encore trop considérables pour garantir une fiabilité constante. La société française Blue Eye ambitionne de « devenir leader mondial de la détection automatique du comportement » ; ses technologies sont pour la plupart développées en partenariat avec l'INRIA (Institut national de recherche en informatique et automatique). Ses systèmes servent au comptage du nombre de manifestants au sein d'un défilé, à la détection de bagages abandonnés, à la surveillance de parkings, à la gestion du trafic routier ; procédures fixées par des critères et paramètres variables *adaptés* à chaque besoin et situation. Durant le pèlerinage de La Mecque en 2005, le groupe Thales a mis en place un « système intégré de gestion de crise », permettant d'optimiser la gestion du mouvement des personnes,

capable de mesurer la densité de la foule et sa vitesse de déplacement grâce à un circuit de trente-deux caméras dont les données étaient analysées en temps réel et gérées par une salle de contrôle qui diffusait des messages sonores appropriés à l'évolution des conditions.

Ce qui caractérise l'évolution de la *matrice*, c'est qu'elle ne se contente plus de saisir les images dans la seule attente d'actes illégaux éventuels, mais qu'elle stocke quantité d'informations relatives aux individus, aussi bien les *constantes* (identification des corps grâce aux technologies biométriques) que les *variables* (activité quotidienne : achats, déplacements, communications, infractions...), traitées par des algorithmes adéquats et mises en relation avec différents serveurs, capables de situer chacun dans l'espace, d'évaluer en temps réel le degré de culpabilité – réel (personnes recherchées) ou virtuel (indices de suspicion) –, ou encore celui du pouvoir et désir d'achat. La puissance panoptique contemporaine ne réside pas tant dans le nombre de dispositifs de vidéosurveillance que dans ses capacités d'analyse et les vitesses de connexion, celles qui *relient* collectes de flux d'informations hétérogènes – dont les images ne constituent qu'une partie – et *bases de données structurées*. « On trouve, dans le programme du Panopticon, le souci de l'observation individualisante, de la caractérisation et du classement, de l'aménagement analytique de l'espace¹². » Néanmoins, à la différence majeure de l'architecture de Bentham, mais selon des fonctions qui en partie se recoupent, l'espace de surveillance ne se restreint pas à celui d'une prison aux contours délimités et à la technologie novatrice, mais à celui d'un horizon *ouvert* et collectif, visé par un *capteur* universel toujours plus omniprésent et *intelligent*.

Un autre type de développement dans l'automatisation de la vidéosurveillance regarde ce qui est nommé « interprétation automatique des images » (*image understanding*), non plus analyse comparative code par code mais combinaison de modèles mathématiques et extraction des données en vue de réaliser une « interprétation » de la scène. LTU Technologies, entreprise multinationale parmi les plus en pointe dans le domaine de la recherche et de la reconnaissance d'images, a notamment inventé le concept d'« ADN de l'image ». Un descripteur visuel classe automatiquement les documents suivant les éléments qui les composent. Pour la vision humaine, images et vidéos revêtent des formes généralement immédiatement identifiables ; pour les processeurs, elles ne représentent qu'une succession de chiffres. Cette technologie, également mise au point en partenariat avec l'INRIA, l'université d'Oxford et le MIT Media Lab, permet à la machine de « percevoir » les données visuelles grâce à un analyseur à forte sensibilité, capable d'indexer, de reconnaître et de comparer des images à partir de leurs composantes. Qu'il s'agisse d'une photographie, d'un dessin ou de toute autre source iconique numérisée, le système produit en temps réel une *description sémantique automatique*. Peut-être viendra-t-il un jour où quantité de

webcams disposées dans les artères urbaines signaleront « par écrit » quelques faits saillants à des unités de contrôle, alors que dans la même zone un homme recevra un texto lui indiquant que son épouse embrasse passionnément le facteur dans leur cuisine, qu'il lui déboutonne son chemisier Zara...

C'est à l'aéroport de Boston qu'avaient embarqué dix des dix-neuf terroristes le 11 septembre 2001. La photographie numérisée de certains d'entre eux avait été fichée, sans que leur déambulation dans les espaces n'ait pour autant déclenché un signal d'alerte. À chaque amélioration des protocoles, des expériences de validation sont mises en place ; à l'occasion de l'une d'elles, 60 % des volontaires n'ont pas été reconnus. Les « taux de rejet » dans l'identification des traits sont encore trop élevés pour favoriser une expansion des systèmes. Jusque-là, il s'est produit un volume ingérable au quotidien pour les services de sécurité à la fois d'arrestations infondées et de « non-reconnaissance » de personnes qui auraient dû l'être. Les critères de distinction d'un visage (lignes supérieures des orbites, zones autour des pommettes, côtés de la bouche, emplacement du nez et des yeux) ne renvoient pas à des modèles invariables. Les traits significatifs pris en compte sont multiples ; les expressions, par exemple, se modifient au cours du temps. La complexité de l'ensemble des paramètres interdit à ce jour une fiabilité, indispensable à l'extension de la reconnaissance automatisée. Un responsable d'une association américaine de droits civils avance qu'il se peut « que le concept soit erroné et que l'identification faciale ne soit que la version XXI^e siècle du détecteur de mensonges, connu pour sa non-fiabilité, bien que certains de ses défenseurs proclament depuis des décennies qu'il fonctionnera un jour ». Cependant, malgré de nombreuses expériences pour le moins aléatoires ou des recommandations contraires émises par divers comités d'experts, quantité de municipalités ou d'instances de sécurité poursuivent leur programme d'acquisition et d'installation de ces dispositifs automatisés.

L'extension ininterrompue de la vidéosurveillance produit encore des effets de confusion entre les dimensions d'espaces *public* et *privé*. L'installation de caméras dans les artères urbaines est souvent légitimée au nom de la protection d'entités privées, celles des commerces par exemple. En France, la « loi antiterroriste » votée fin 2005 « autorise la vidéosurveillance dans les transports collectifs, les abords des gares et ceux de différents lieux accueillant du public : commerces et lieux de culte ». L'urbanité contemporaine, toujours plus structurée par des logiques de *shopping*, tend à confondre les distinctions historiques entre zones réservées au commerce et celles relevant de l'habitat ou de la collectivité, entendues comme lieux de rencontre, de rassemblement et de libre déambulation. Depuis le début des années quatre-vingt-dix, plusieurs urbanistes, architectes, sociologues observent et analysent ces phénomènes de *marchandisation* de l'espace. Suite au fameux *Learning from Las Vegas* de Robert Venturi et Denise Scott Brown, et aux théories de John Jerde sur l'importance des lieux de négoce

dans l'évolution historique des cités, Rem Koolhaas a développé un corpus capital relativement à l'expansion du shopping et ses multiples incidences¹³. Je renvoie également à l'ouvrage de l'architecte David Mangin, *La Ville franchisée*¹⁴, qui examine l'élargissement du principe de délégation de service public à des entreprises privées qui induit une pénétration progressive de schémas prioritairement déterminés par le souci du profit dans l'élaboration et la réalisation de programmes urbains ou la gestion d'équipements sportifs, de loisirs ou culturels. L'architecte britannique Richard Rogers, très soucieux de la préservation et du développement des espaces ouverts de socialité, affirme pour sa part : « Nous devons défendre la liberté de l'espace public avec la même détermination que la liberté d'expression¹⁵. »

La privatisation continue de l'espace public¹⁶ produit plusieurs effets insidieux qui bouleversent considérablement une situation jusque-là nettement découpée entre responsabilités, dévolues d'un côté au politique et de l'autre à l'économique. Elle brouille d'abord les cadres juridiques censés se rapporter à certains types de territoires, elle perturbe ensuite les critères qui président à l'emplacement des dispositifs de surveillance, elle modifie enfin une large part des types de personnes, supposées décider de leur installation. La « loi antiterroriste » française de 2005 favorise exactement ces jeux de transfert, ou de « délégation », à des petits commerçants par exemple, légalement qualifiés à placer des caméras sur des artères *publiques* autour de leurs boutiques. Il s'opère une double impulsion qui favorise encore une extension de la vidéosurveillance, soutenue à la fois par des citoyens angoissés mais *autorisés* à *densifier* la grille et par des élus tout autant angoissés par la pression des mêmes citoyens, à laquelle ils s'efforcent de répondre à l'aide d'équipements électroniques, perçus comme aptes à calmer ces anxiétés généralisées.

Un nombre croissant d'établissements scolaires (publics et privés) disposent dans leurs locaux de caméras, en vue d'un but déclaré prioritaire : la protection des équipements et du matériel. L'aggravation des violences entre élèves et entre élèves et professeurs, qui parfois conduit à des actes extrêmes, a encore encouragé un récent développement de la vidéosurveillance en milieu scolaire. La prolifération du nombre de circuits vidéo est encore favorisée par la généralisation de la « vidéosurveillance IP » (via Internet), qui rend ses modes d'utilisation plus souples et légers. Sa légèreté logistique et technique facilite les possibilités de mise en place et d'usage à l'intention d'organismes publics ou privés. Également à l'intention d'individus capables d'installer à des coûts toujours plus faibles des mini-caméras au sein de leur habitat, de les visionner ou de les piloter à distance, ou encore d'être alertés par la réception de SMS ou emails de l'intrusion d'un corps à l'intérieur d'un espace (une maison inhabitée durant une période de vacances, par exemple), induisant encore une expansion d'une *vidéosurveillance horizontale* entre personnes, stimulée par la *miniaturisation* et la *portabilité* des dispositifs techniques contemporains.

Équilibres instables

La mise en place de circuits vidéo procède de plus en plus de décisions impulsives, prises sans examen préalable de la *pertinence* de l'objet, relativement aux spécificités d'un territoire ou des objectifs visés. Il reviendrait à la responsabilité des pouvoirs publics de définir certains critères rigoureux, aptes à prendre en compte l'ensemble des caractéristiques propres à un environnement singulier. L'installation d'un dispositif devrait être soumise à un processus d'approbation préalable par une autorité indépendante, ce qui n'est pas le cas en France par exemple, où elle est subordonnée à une autorisation délivrée par le préfet, après avis d'une commission départementale présidée par un magistrat. (Les espaces privés dépendent d'une autorisation de la CNIL.) L'expansion parfois injustifiée de circuits vidéo modifie selon des termes renouvelés l'équation entre exercice des libertés publiques et préservation de l'ordre commun – impératifs souvent jugés antinomiques –, qui peut conduire à une tension avec les textes constitutionnels. Le « principe de proportionnalité », censé représenter une garantie à l'égard de la vie privée, est tout autant susceptible d'être renversé : un juge administratif peut y avoir recours afin d'autoriser l'installation de caméras, au nom de la sécurité d'une zone jugée potentiellement menacée. Cet équilibre entre deux exigences fondamentales demeure en France très instable, soumis en partie à des appréciations subjectives et non pas à quelques critères prioritaires et irréductibles, à l'instar de l'*Habeas Corpus* britannique datant de 1679, dont l'objectif majeur consiste à garantir *avant toute chose* la liberté individuelle.

Une architecture juridique stricte encadre néanmoins l'usage de la vidéosurveillance en France, mais conçue et rédigée sur cette balance incertaine, capable de légitimer des excès au nom de la primauté accordée à la « discipline sociale ». La tension entre droit fondamental à la vie privée et exigence collective du « maintien de l'ordre » est encore appelée à être radicalisée par la conjonction de deux facteurs : 1/ développement et sophistication de techniques aux capacités toujours plus *intrusives* ; 2/ environnement social troublé et situation internationale marquée par la menace terroriste virtuellement omniprésente. Il devient presque inévitable que s'opère une *torsion* sur le champ légal, davantage constitué en vue de garantir la sécurité publique que de se soucier *simultanément* ou *indissociablement* du droit de chaque individu à disposer comme bon lui semble des données récoltées qu'il dissémine consciemment ou non, et qui engagent une large part de ce qui est nommé « vie privée ». Le croissant déséquilibre opéré par le législateur, au profit du « bien commun » et au détriment du souci de l'intégrité individuelle, renvoie depuis le 11 septembre 2001 à un schéma géopolitique qui se déploie, certes selon des degrés d'intensité variables suivant les continents et les pays, mais qui correspond néanmoins à une forte *tendance* historique contemporaine. Le positionnement

des États-Unis exposerait (avec celui de la Chine) les pics d'un diagramme planétaire (notamment par le fait des dispositifs juridiques Patriot Act I & II¹⁷) destinés à contenir la nébuleuse terroriste (ennemis plus ou moins exogènes) ; alors que l'obsession chinoise regarde la conservation d'un ordre politique unique et omnipotent (menace endogène).

L'Europe, malgré sa réputation « tempérée », s'inscrit progressivement à l'intérieur de cette propension à favoriser le supposé « intérêt général » au détriment de celui dû au particulier, déclaré depuis les Lumières comme étant en fait et en droit absolument inaliénable. En France, la « loi antiterroriste » de 2005 induit exactement ce type de glissement, et trouve ses conditions d'adoption à l'intérieur d'un environnement frappé depuis septembre 2001 par une rupture qui a modifié la perception commune de cet ordre historique s'efforçant d'entrelacer au mieux code communautaire et autonomie individuelle. Une nouvelle *schizophrénie* infiltre désormais les consciences, déchirées à accorder des principes parfois opposés ou en partie inconciliables. C'est encore cette double axiomatique qui change radicalement la donne – technologies à l'œuvre au champ de visée et d'*analyse indifférenciés*, et le fait d'*ennemis sans visage*, à la localisation incertaine et mouvante –, qui reconfigure du tout au tout l'architecture générale de la surveillance contemporaine, situant le législateur sur des territoires fragiles, appelé *soit* à maintenir la sauvegarde de valeurs historiques, *soit* à offrir aux États les moyens de les prémunir de dangers estimés comme étant désormais *omniprésents*.

L'universalité et la virtualité de la menace altèrent une dimension jugée irréductible et fondatrice de l'individu moderne : le droit de protéger sa vie privée. Mais le constat serait encore trop compact relativement à la complexité de la situation. C'est, à coup sûr, la notion même de « vie privée » qui est bouleversée, celle supposant jusque-là une série d'activités dont la socialité admet délibérément qu'elles ne peuvent faire l'objet d'une attention collective, car elles relèvent d'une dimension *absolument* propre¹⁸. Le registre répertorié comprend la vie menée dans l'habitat, les relations amicales et amoureuses, les pratiques sexuelles, les achats, loisirs, voyages, bref des actions dont la décision appartient à chacun, à condition de ne pas enfreindre la loi, ce qui ne peut être vérifié qu'*a posteriori*. Or, à y regarder de près, la totalité des actes signalés font maintenant l'objet d'une *vigilance*, permise par l'association de technologies de *traçage*. Il s'opère un *glissement* de la valeur accordée à la notion, sous la forme d'un rétrécissement de ses délimitations, d'une perte de terrain progressive, ou plus précisément encore d'une insidieuse *hybridation* de son régime, à la fois relevant d'une spécificité sociale, éthique et juridique, et perçue depuis peu comme devant nécessairement *s'exposer* – d'une façon plus ou moins déclarée ou légale – aux yeux et à l'« intelligence » des dispositifs de suivi.

L'« objectif » se focalise sur cette zone historiquement « à l'abri » et

amplifie peu à peu la « puissance du zoom » découvrant un territoire jusque-là préservé, maintenant soumis aux pouvoirs d'analyse des processeurs électroniques. Procédures légitimées par le risque diffus, qui oblige à agir presque sans repères, à promulguer des décrets supposés renforcer l'ordre sécuritaire mais non sans effets collatéraux sur les structures démocratiques : « L'état d'exception n'est pas une dictature (constitutionnelle ou inconstitutionnelle, de commissaire ou souveraine), mais un espace vide de droit, une zone d'anomie où toutes les déterminations juridiques – et avant tout la distinction même entre public et privé – sont désactivées¹⁹. » Dans le film *Ennemi d'État* (*Enemy of the State*), réalisé en 1998, avant donc le 11 Septembre, par Tony Scott, on voit la NSA (National Security Agency) utiliser un large spectre de technologies et de pratiques (vidéosurveillance omniprésente, interceptions des communications, analyses de données, GPS, biométrie...), et lutter farouchement contre tous ceux qui s'opposent à l'intensification des procédures de contrôle. Un des enjeux du scénario vise à exposer l'inquiétante *vulnérabilité* qui règle la tension entre exigences démocratique et sécuritaire. Une scène montre un député affirmant sur une chaîne d'information en continu : « Surveillance et liberté sont en équilibre fragile, quand les immeubles sautent, les priorités changent » ; quelques scènes plus tard, le responsable jusqu'au-boutiste de la NSA, interprété par Jon Voight, lui répond en écho : « Le droit privé c'est fini : trop risqué. »

Les modalités de fonctionnement de la vidéosurveillance se sophistiquent sans cesse suivant deux constantes majeures : d'une part, les mécanismes se miniaturisent et *s'intègrent* ou fusionnent toujours plus « harmonieusement » avec les surfaces physiques, par phénomènes de discrétion, tendant à l'avenir vers encore plus de « transparence ». D'autre part, les capacités de traitement des données iconiques, malgré les défaillances que nous avons décrites, s'amplifieront et se perfectionneront, non seulement par augmentation de puissance des calculs, mais surtout par une amélioration de la pertinence des analyses – grâce aux perfectionnements de l'*intelligence artificielle* –, dotant les yeux électroniques de pouvoirs de reconnaissance des visages et d'identification des comportements bien plus précis qu'ils ne l'auront été lors de la première décennie du XXI^e siècle. L'expansion continue du nombre de caméras dans l'environnement contemporain induit un scannage systématique et *indifférencié* des corps, dont les mouvements produisent des lignes de codes destinées à évaluer le degré de *dangerosité* de chacun à l'intérieur d'une « grille » universelle et sans rupture. Cette architecture dessine à coup sûr un nouveau paradigme, au sujet duquel il reste possible d'espérer que seuls des cadres juridiques sévères autant qu'une attention soutenue et structurée des citoyens pourront atténuer une *intrusivité* sans limite. Les textes législatifs, pour la plupart réduits à des cadres nationaux, ou pour l'Europe à hauteur de l'Union, supposent au sein de notre monde global des différences territoriales et des oppositions géopolitiques qui complexifient l'ambition d'un

contrepoids légal international et homogène.

Il existe certes des formes de vigilance formalisées par la publication de revues, d'articles, de sites Internet, à l'instar de l'association « Souriez vous êtes filmés²⁰ » qui indique, selon ses termes, être constituée « depuis 1995 par un collectif de personnes désireuses de ne pas sombrer dans une société de technologie répressive et de proposer des alternatives militantes festives. Elle s'est donnée comme but le retrait des caméras de vidéosurveillance, et entend être un lieu de regroupement humain pour débattre de la société dans laquelle nous souhaitons vivre. [...] Elle organise des actions (masquage de caméras) [...], et entreprend également des recours juridiques visant à supprimer les caméras de surveillance ». Cette déclaration serait emblématique d'attitudes tendanciellement louables, déterminées par une sorte de « veille citoyenne » structurée au sein d'une entité publique et ouverte, mais à y lire de plus près, fondée sur quantité d'*a priori* erronés. Il s'opère d'entrée une corrélation de l'ordre de l'évidence entre « technologie » et « répression », qui estime que les outils commandent les actions, alors que ce sont les usages qui *ajustent* et règlent les objets.

On suppose comme entendue l'opposition entre machines et hommes, conformément à une longue filiation qui prend son origine dans Platon, reprise par Rousseau, prolongée par Heidegger et plus récemment par Debord, pour lesquels la « prothèse technique » représente un *supplément* insupportable – phénomène précisément analysé par Jacques Derrida dans *De la grammatologie* –, et perçu comme une déviation, une « erreur de parcours » ou une déficience anthropologique, contre lesquelles il faudrait lutter en vue de retrouver une « plénitude de l'être », sorte de présence à soi-même et aux autres non médiatisée et coordonnée par des « liens directs ». Est-il vraiment nécessaire de signaler la naïveté de ces positions qui en appellent toujours à « l'humain », érigé comme un concept métaphysique autonome, qui aurait dû rester à l'abri des corruptions de l'histoire et dont on devrait reconquérir le fantasmatique noyau fondamental et invariable ? André Leroi-Gourhan fut le premier à s'opposer à ces illusions, avec les arguments démontrables de la paléontologie, qui permettent de suivre au plus près les « cheminements » de l'hominidé, à la fois soumis à des transformations corporelles et cérébrales successives et « ancré » dans son milieu par des immixtions continues modifiant la nature et les pouvoirs du geste : « La liberté de la main implique presque forcément une activité technique différente de celle des singes et sa liberté pendant la locomotion, alliée à une face courte et sans canines offensives, commande l'utilisation des organes artificiels que sont les outils. Station debout, face courte, main libre pendant la locomotion et possession d'outils amovibles sont vraiment les critères fondamentaux de l'humanité²¹. »

L'enjeu ici ne consiste pas à reprendre les nombreux préjugés idéologiques tronqués, fondés sur des schémas binaires et sur le mythe d'une humanité qui se serait « égarée » dans la technique. Je renvoie à Gilbert Simondon, trop

longtemps occulté et qui rencontre depuis une dizaine d'années un intérêt, qui pourra contribuer à complexifier autant que possible les modalités de perception relatives aux interactions entre individus et environnements artificiels : « La culture s'est constituée en système de défense contre les techniques ; or, cette défense se présente comme défense de l'homme, supposant que les objets techniques ne contiennent pas de réalité humaine. Nous voudrions montrer que la culture ignore dans la réalité technique une réalité humaine. [...] L'opposition dressée entre la culture et la technique, entre l'homme et la machine, est fausse et sans fondement ; elle ne recouvre qu'ignorance ou ressentiment. Elle masque derrière un facile humanisme une réalité riche en efforts humains et en forces naturelles, et qui constitue le monde des objets techniques, médiateurs entre la nature et l'homme²². »

La proclamation de « Souriez vous êtes filmés » s'inscrit encore à l'intérieur d'un large mouvement qui affirme positionner le cadre de ses actions à l'intérieur de logiques de « résistance ». Outre que l'usage d'un tel vocable appelle la plus grande prudence, il suppose surtout une attitude d'opposition radicale qui réduit un horizon composé de situations variables et spécifiques à un ensemble compact, *de facto* jugé néfaste, suivant un *a priori* doctrinal surdéterminant. Alors que la complexité des structures globales et locales appelle l'exigence d'une analyse informée et construite *au cas par cas*, et soucieuse de prendre en compte la multiplicité des enjeux sociaux, géopolitiques, légaux, éthiques. La notion de « résistance » telle qu'elle est souvent brandie par les « mouvements citoyens » contemporains opère une sorte de crispation figée sur quelques postulats ou principes humanistes, au sujet desquels chaque être de raison pourrait souscrire mais dont les ennemis identifiés et les solutions envisagées se situent à l'intérieur de registres qui catégorisent toujours les « dominants » d'un côté (pouvoirs politiques, chefs d'entreprise, chercheurs innovants²³, responsables de groupes de presse... – exemples pris ici parmi les plus emblématiques et les plus récurrents), et d'un autre côté les « dominés ». Ces logiques dichotomiques ont contribué à étendre l'illusion selon laquelle il suffit d'extirper le « Mal » à l'œuvre au sein d'une situation pour finalement la résoudre, à pointer des raisons massives et exclusives, à l'écart de la formule de Max Weber pour qui il n'existe jamais de cause unique à tout phénomène.

Un des défis de notre temps regarde notre capacité à développer des modes d'analyse et d'action fondés sur une capacité à évaluer « localement » – à l'intérieur d'un environnement épistémologique global – les caractéristiques propres à chaque configuration, en vue de sélectionner certaines de ses structures, de les *recomposer*, ou d'en convoquer de nouvelles, suivant des jeux constructifs variables en fonction de chaque « complexité spécifique ». Les pratiques artistiques représentent, à mon sens, un champ d'intervention susceptible de mettre en place des stratégies *subjectivées* et pragmatiques par l'élaboration de *dispositifs* envisagés comme des *cas de figure singuliers*,

appelés à faire pivoter plusieurs types d'enjeux à partir d'une *focale précise*. « Au lieu de s'opposer à cet état de conditionnement, au lieu de le dénoncer, on peut user de ses dispositifs. Bruce Nauman est le premier à avoir créé des installations en circuit fermé pour les détourner. *Live / Taped Video Corridor* (1969-70) unit une caméra de surveillance à l'entrée d'un couloir et deux moniteurs à son extrémité. Le spectateur, filmé de dos, de face ou sur le côté, pendant qu'il avance, est renvoyé à un dé-centrage de sa perception, entre sa progression et l'image contradictoire des moniteurs. S'attachant aussi à l'étude approfondie des mécanismes de la perception visant à l'identification, au repérage, donc à la surveillance²⁴. »

Bruce Nauman, dans le cadre d'un autre travail, *Video Surveillance Piece : Public Room, Private Room* (1969-70), installe au sol et dans un coin un moniteur. Le spectateur découvre que l'écran ne diffuse pas comme il pourrait s'y attendre les images des personnes présentes mais celles d'une autre pièce mitoyenne et inaccessible : une « *Private Room* » qui diffuse, elle, probablement les images de la salle publique, selon des usages dissimulés et méconnus, qui ne peuvent que susciter interrogations et inquiétudes. Ici une tactique de *focalisation* est privilégiée qui vise à exposer, à l'intérieur d'un lieu concentré, certains des mécanismes à l'œuvre dans la vidéosurveillance : être pris à son insu et diffuser son image dans un espace et un temps déterminés, dans l'ignorance de l'identité des personnes qui recueillent les informations et des utilisations qui en sont exactement faites. *Time Delay Room* (1974), de Dan Graham, dispose deux salles ouvertes l'une à l'autre, chacune comprend deux écrans et une caméra accrochée au plafond. Dans chaque pièce, sur l'un des deux moniteurs, le public voit en direct les personnes situées dans l'autre pièce ; sur l'autre écran, il se voit dans la pièce qu'il occupe, mais avec un décalage temporel de huit secondes. « La désynchronisation des temps et le dédoublement de la figure du spectateur ou du regardeur en regardeur/regardé brouillent les pistes : on est à la fois le surveillant et le surveillé, le veilleur et le veillé. Continuité temporelle, séparation spatiale, impossibilité de (tout) voir... On retrouve bien ici les composantes essentielles du dispositif de vidéosurveillance, à une nuance près, mais de taille : on entre et on sort du dispositif comme on l'entend, on y joue plusieurs rôles²⁵. »

Le *glissement* des fonctions et des rôles constitue l'enjeu central de la pièce, impliquant notamment une dimension de voyeurisme ludique ; dimension aujourd'hui amplifiée par la miniaturisation des objets numériques, qui généralise les phénomènes d'individualisation de la surveillance contemporaine. Denis Beaudois, par exemple, a développé des stratégies plus frontales, consistant à se poster dans l'espace public face à des caméras et à exhiber des panneaux sur lesquels il était notamment écrit : « *Move the camera up & down to agree* », à l'occasion de performances de plusieurs heures intitulées *In the Event of Amnesia the City Will Recall*, *Sydney & Cleveland Performances*. L'objet de notre recherche ne consiste pas ici à

retracer une généalogie ou un panorama actuel d'expérimentations artistiques, mais à signaler au passage l'*efficace* possible de certains agencements destinés à faire partager une *expérience*, dont une des valeurs consiste à pointer, ou à faire éprouver par le *corps*, quelques processus ou conséquences en jeu à l'occasion de la « traversée » d'un dispositif de surveillance, et de susciter des *effets de conscience* à l'écart de logiques discursives dénonciatrices.

La vidéosurveillance fait aujourd'hui l'objet d'une méfiance et d'une peur généralisées, probablement par sa capacité de « vision » autonome, qui personnalise presque le procédé et induit une dimension anonyme, inquiétante et virtuellement omniprésente. Néanmoins, cette angoisse se leurre par le fait d'un trop grand privilège accordé à la partie visible des dispositifs et qui occulte les processus déterminants qui se mettent en place depuis plusieurs années, qui se développent et s'affinent sans cesse, selon des modalités *invisibles* et aux formes quasi immatérielles : l'articulation de l'ensemble des techniques de traçabilité à des *bases de données*. L'avenir dessine une gigantesque *maille interconnectée* physiquement incontournable : la totalité des moyens de *repérage* ou d'*identification* (vidéosurveillance, biométrie), de *localisation* (satellites + récepteurs ; capteurs + puces électroniques), d'*élaboration de profils* (dissection des comportements : communications, achats, déplacements...), est connectée à des serveurs stockant des « océans informationnels » *traités* par des algorithmes adéquats, au pouvoir toujours plus *intrusif*, grâce aux développements de l'intelligence artificielle et de l'industrie des composants électroniques – dont l'horizon dessine déjà les dimensions *quantique* et *nanotechnologique*.

La structure de la surveillance contemporaine n'est plus constituée d'isolats épars mais expose une *architecture universelle en réseau*, qui *collecte* les *traces* et les *analyse*. Une interrogation présente et à venir décisive renvoie au volume d'*interopérabilité* qui sera déployé entre les bases de données qui restent à ce jour la propriété d'instances étatiques ou de groupes privés, qui certes échangent ou cèdent déjà une partie de leurs informations suivant des méthodes souvent illégales, mais qui restent *encore* soumises à des contraintes. Un environnement de nature technique et anthropologique tout autre se constituera lorsque la loi, les États, les entreprises autoriseront et opéreront peu à peu (de gré ou de force) une *agrégation* achevée des données, arme du XXI^e siècle impitoyable, disponible aux pouvoirs politiques et économiques qui instaureront, non pas un panoptique uniquement chargé de *surveiller* (forme historique désormais désuète), mais une *matrice intelligente intégrale* destinée à *quantifier* les individus et à *anticiper* la plupart de leurs actions, qu'elles relèvent d'un danger potentiel (sécurité) ou de *désirs* éventuels (marketing) : « Notre objectif est de traiter toutes les bases de données éparpillées dans le monde comme un seul fichier²⁶. »

- 1- Michel Foucault, *Surveiller et punir*, Paris, Gallimard, 1975, p. 234-235.
- 2- Propos rapportés par Marie Lechner, in « Ars Electronica, le doyen des festivals d'arts électroniques, scrute la fièvre sécuritaire qui nous encercle », *Libération*, 10 septembre 2007.
- 3- Cf. notamment *Metapolis*, Paris, Odile Jacob, 1995 ; *La Société hypermoderne. Ces événements nous dépassent, feignons d'en être les organisateurs*, Paris, Éditions de l'Aube, 2004.
- 4- Sur les questions en rapport avec une forme d'autonomie des développements techniques, cf. particulièrement : Jacques Ellul, *Le Système technicien*, Paris, Le Cherche Midi, 1977.
- 5- Michel Foucault, *Surveiller et punir*, *op. cit.*, p. 236.
- 6- *Surveiller et punir*, *op. cit.*, p. 235.
- 7- George Orwell, *1984*, Paris, Gallimard, « Folio », p. 148.
- 8- Film de 2004.
- 9- Réalisé en 2002 par Roger Donaldson.
- 10- D'Adam Rifkin (2007).
- 11- Cf. mon ouvrage *Times of the signS* (Birkhäuser, 2007), dans lequel j'explore la complexité de la société de l'information contemporaine, notamment l'extension sans fin d'*écrans* dans notre environnement quotidien.
- 12- Michel Foucault, *Surveiller et punir*, *op. cit.*, p. 237.
- 13- Cf. particulièrement : Rem Koolhaas, *S, M, L, XL*, Monacelli Press, 1995.
- 14- David Mangin, *La Ville franchisée (formes et structures de la ville contemporaine)*, Paris, Éditions de la Villette, 2004.
- 15- Richard Rogers, *Leith Lecture Conference*, Londres, BBC, 1995.
- 16- Sur cette question, cf. l'ouvrage décisif d'Evan McKenzie, *Privatopia : Homeowner Associations and the Rise of Residential Private Government*, Yale University Press, 1996.
- 17- « La section 213 de l'USA Patriot Act autorise les agents policiers fédéraux à "pénétrer subrepticement pour jeter un coup d'œil" chez les citoyens. Cette nouvelle pratique déjà généralisée et baptisée "*sneak and peek*" est, elle aussi, annonciatrice d'une nouvelle ère où non seulement la surveillance est la norme, mais où l'individu est tenu de se taire et de s'y plier. Les effractions dans l'espace privé se font dorénavant de préférence en son absence et sans que le geste civique de le prévenir soit effectué » (Robert Harvey et Hélène Violat, *USA Patriot Act, de l'exception à la règle*, *op. cit.*, p. 38-39).
- 18- Jeffrey Ullman, spécialiste américain du *data mining* (fouille de données), estime que « le monde a changé et [que] la notion de protection de la vie privée doit évoluer en conséquence ». Cité par Jacques Henno, in *Tous fichés, l'incroyable projet américain pour déjouer les attentats terroristes*, Paris, Éditions Télémaque, 2005, p. 34.
- 19- Giorgio Agamben, *État d'exception, Homo Sacer*, Paris, Le Seuil, 2003, p. 86.
- 20- <http://souriez.info>.
- 21- André Leroi-Gourhan, *Le Geste et la Parole, technique et langage*, Paris, Albin Michel, 1964, p. 33.
- 22- Gilbert Simondon, *Du mode d'existence des objets techniques*, Paris, Aubier, 1958, p. 9.
- 23- Cf. les *réactions* suscitées par l'inauguration à Grenoble de l'Imantec, centre de recherche dédié aux nanotechnologies ; les « actes de résistance » consistaient à dénoncer les menaces possibles de surveillance des citoyens, suivant une perception paranoïaque et toujours jugée hostile envers les innovations technologiques. Il va de soi que la manipulation de l'échelle nanométrique va modifier à terme nos rapports à l'environnement physique et amplifier, par exemple, les capacités d'analyse des mouvements des corps ; cette disposition constitue *une* des perspectives possibles de développement. L'enjeu ne peut en aucune manière consister à s'opposer à ces explorations dans leur ensemble, mais à encadrer légalement certaines fonctionnalités annoncées, à veiller avec vigilance aux dispositifs à venir, sans nier la positivité possible de configurations techniques inédites.
- 24- Louis-José Lestocart, « Aporie sur l'enfermement », *Art Press*, n° 303, juin 2004.
- 25- Christophe Kihm, « Vidéosurveillance et identité, les modalités de la présence », *Art Press*, n° 303, juin 2004.
- 26- Affirmation de l'amiral américain John Poindexter, ancien responsable du projet « Surveillance totale », cité par Jacques Henno en préambule de son ouvrage : *Tous fichés. L'incroyable projet américain pour déjouer les attentats terroristes*, *op. cit.*

IV

BASES DE DONNÉES

Récolter / analyser / alerter

Les chiffres et les choses

Les pouvoirs politiques – historiques ou contemporains – supposent d’une façon consubstantielle à leur assise un rapport *paranoïaque* à l’environnement ; d’abord à l’égard des « cénacles » (toujours susceptibles de critiques déstabilisantes ou d’intrigues malveillantes) ; ensuite à l’égard des populations sous autorité (maintien d’un ordre jamais définitivement acquis) ; enfin à l’égard d’ennemis exogènes plus ou moins déclarés (espionnage/contre-espionnage). La crainte des différents dangers pousse à la *récolte* de renseignements relatifs aux personnes, à leur *classification*, à leur *archivage*, ainsi qu’à un usage structuré adapté aux besoins : gestion rationalisée de l’entité sociale ; prévention de menaces possibles ; recherche efficace de personnes soupçonnées. Chaque individu doit être identifié avec la plus grande précision : nom / date et lieu de naissance / ascendance familiale / description physique / lieu d’habitation / activités ; caractéristiques qui représentent des constantes transhistoriques – adjointes à d’autres types d’informations selon les siècles et les territoires. L’établissement de fichiers représente une dimension indissociable de la relation entre le Prince et le peuple, qui a régulièrement évolué en fonction des différentes techniques d’écriture et de mémorisation, qui ont au fur et à mesure modifié les modes de *saisie*, d’après une courbe toujours ascensionnelle amplifiant volumes de conservation et perfectionnement taxinomique des individus. Notre souci ne consiste pas ici à établir une longue généalogie du rapport entre sécurité et recueil des données, mais à relever à quel point l’évolution des *prothèses mnémotechniques* a permis une sophistication continue des usages, grâce à une *maniabilité* plus aisée, à l’*accélération* et à l’*affinement* des traitements des renseignements. L’annotation sur des tablettes d’argile, la constitution de registres imprimés, l’apparition de cartes perforées et autres innovations successives au cours de l’histoire ont considérablement accru la *visibilité cartographique* du corps social¹.

« La chute du Mur, en Allemagne, a entraîné la découverte de l'extraordinaire activité scripturale dont a été accompagnée la surveillance dans les pays de l'Est. [...] Opérations d'archivage qui ont fini par constituer dans l'ancienne République démocratique allemande un fonds de cent quatre-vingts kilomètres de dossiers. Photographie kafkaïenne d'une société surveillée². » Monde clos renfermant cartons et papiers empoussiérés, appartenant à une période somme toute récente mais en tout point révolue. Les gigantesques volumes contemporains de stockage informationnel ne se *fixent* plus au sein d'agencements physiques, mais sont le résultat exclusif de traitements électroniques *dynamiques* qui revêtent une nouvelle dimension *immatérielle* et *invisible*. L'expansion de l'interconnexion s'inscrit dans le prolongement de cette longue archéologie du classement technicisé, et à la fois brise tout effet de continuité par l'installation d'une architecture sans commune mesure, due au fonctionnement incomparable des technologies numériques exclusivement fondé sur des processus computationnels, qui réduisent l'ensemble des objets analysés à des séquences de chiffres, suivant un mécanisme qui fractionne chaque fait en détails infimes produisant une mise à plat haute définition et systématisée d'ensembles informationnels initialement plus ou moins compacts. Le bit est l'équivalent du pixel : une particule élémentaire qui, reliée à d'autres particules, produit des fichiers dont la cohérence et la précision sont rendues possibles par un traitement quantifié en millions ou en milliards d'unités. Le numérique se constitue sur une procédure de *décomposition* des éléments en une infinité de fragments standardisés, et de recombinaison suivant les algorithmes déterminés. Il transforme toute réalité factuelle en *données*, instaurant un rapport médiatisé aux êtres et aux choses, par des séries de 0/1 *manipulables*, imposant désormais une couche à notre perception, non plus réglée sur la représentation mais sur la *quantification*. Notre relation à l'environnement est en continu interférée par des opérations électroniques qui induisent une intelligence intériorisée de notre milieu comme étant en tout point innervé par des codes, à l'instar de la matrice globale qui enveloppe la « réalité » exclusivement composée de chiffres à l'œuvre dans la trilogie *Matrix* réalisée par les frères Wachowski.

La structure du numérique autorise non seulement une optimisation en termes de gestion des volumes et de vitesse des traitements, mais permet également des fonctionnalités augmentées : faculté de *conjuguer* entre eux des régimes symboliques distincts ; réduction indifférenciée de documents hétérogènes à des codes chiffrés (de nature textuelle, iconique, sonore) ; *pliage* des données en fonction des logiciels utilisés ; repérage et *marquage* automatisés de l'information ou « indexation » (grâce à l'intelligence artificielle) ; puissance sans cesse croissante de stockage sur les disques durs... La multiplicité des usages et manipulations possibles, ainsi que les capacités d'accès à distance et de transmission, constituent un *saut historique* dont l'avènement instaure une réalité désormais achevée : la conception et

l'élaboration d'*atlas planétaires des identités* standardisées. Radiographies informationnelles dressées par des personnes ou des groupements *en quête d'autrui*, exécutées par des *robots électroniques* à la force de pénétration et d'intrusivité fondée sur la vitesse de la lumière et la parcellisation de tout élément du réel à l'échelle de fractions indivisibles et microscopiques.

Ce qui caractérise prioritairement les fonds informationnels numériques (*databases*) renvoie à la capacité qui leur est associée d'*analyser* en « temps réel » les agrégats de données, de les « interpréter » au sein de multitudes, de *détecter* des significations, aussi bien relativement à des ensembles constitués qu'à l'égard de masses indifférenciées « visitées » suivant les besoins ou les indices collectés. Les développements des systèmes électroniques de modélisation des langues naturelles ont permis d'inscrire l'*indexation automatique* comme un mécanisme majeur de la société de l'information contemporaine (emblématique dans les moteurs de recherche, par exemple), et comme une arme de repérage et d'identification des séquences de codes, apte à produire une *distribution des renseignements* suivant des classifications rationalisées et des cartographies mobiles des êtres ou des choses, dont la « profondeur de champ » est infiniment amplifiée par la captation automatisée des signes, d'après les séries de chiffres qui les désignent et les programmes décidant ou non de leur sélection et de leur « sauvegarde ».

Le futur fantasmé au cours des années cinquante et soixante, peuplé de robots animant les espaces de travail et les intérieurs domestiques, n'a finalement pas connu une réalisation généralisée (seulement partielle dans les chaînes de montage), mais s'est finalement accompli autrement, sous la forme dématérialisée d'*agents incorporels* et volatils circulant le long des réseaux numériques, configurés grâce aux statistiques, probabilités et constantes dégagées par l'intelligence artificielle. Une forme de quasi-perfection du repérage et de l'analyse de l'information (donc des personnes) se confirme et se développe en ce début du XXI^e siècle, qui se substitue en partie au suivi physique des corps et de leur représentation dans l'espace, au profit d'un glissement progressif vers leur *quantification* ; identités non plus ordonnées selon leurs noms et leurs mouvements sur des cartes, mais *signalées* suivant des *codes* et des *liens* sur des *plans virtuels* ; virtualité entendue non seulement dans la dimension constamment évolutive des « états de fait » ou des « profils », mais plus encore dans l'aptitude ouverte à les *distribuer* en fonction des différents usages et objectifs visés.

Une base de données électronique pourrait être ainsi définie : masses d'informations sous formes de codes numériques, stockées sur des disques durs « fermés » ou sur des serveurs connectés, classifiées selon des catégories, indexées et offrant des modalités d'accès structurées. D'une certaine façon, la quasi-totalité des identités et des actions se *convertissent* aujourd'hui en *diagrammes* disponibles (état civil des individus, Sécurité sociale, fiches

d'imposition, dossiers médicaux, achats par cartes de crédit, comptes bancaires, abonnements à divers services, transports effectués...). Il serait difficile d'isoler des types d'activités qui ne produisent pas des séries de chiffres : peut-être une promenade en forêt, néanmoins un téléphone portable allumé induit un suivi continu par les antennes relais, phénomène qui sera renforcé par l'intégration de systèmes de géolocalisation (GPS ou Galileo) aux multiples protocoles miniaturisés portables et interconnectés. En outre, l'expansion des étiquettes radio (*tags RFID*, sur lesquels nous reviendrons) et l'introduction de puces dans les corps, détectées par des capteurs à l'avenir presque omniprésents, autoriseront une dissection systématique et « sans rupture » des corps et des gestes. La récolte informationnelle contemporaine est encore appelée sans cesse à se densifier par l'accroissement continu et simultané des puissances de calcul et des capacités de stockage. L'individu hypermoderne opère bon gré mal gré, lucidement ou aveuglément, une *dissémination* infinie de ses *traces*. Là où Jacques Derrida, dans *La Dissémination*³, analysait les conditions de prolifération et de circulation de l'écrit comme le signe patent d'un *excès* perturbant et *débordant* sans fin les bornes fixées du logos classique, le *traçage numérique*, lui, génère les spasmes sournois qui désormais bouleversent et *débordent* le cadre légal et social esquissé et développé depuis les Lumières, relatif à l'intégrité de la personne, de son droit à la vie privée, celui de pouvoir situer une part irréductible de son existence *absolument* en retrait de tout examen public.

L'individu réduit à des codes ?

Le concept de « corps sans organe » développé par Gilles Deleuze, entendu comme une légèreté délibérément affranchie du poids des surdéterminations familiales et névrotiques, déployant son énergie à susciter la traversée d'expériences intenses, provisoires et changeantes, se trouve aujourd'hui, d'une certaine façon, « transféré » au sein de l'architecture globale qui compose la collecte universelle d'informations auprès des individus, réduisant les traces éparpillées par chacun au statut – celui-ci non métaphorique mais bien factuel – de *corps sans organe stockés sur des serveurs*. Les gestes (achats, déplacements, situation médicale...) produisent des codes qui génèrent un *dédoublement* de chaque personne sous la forme de *calques virtuels*, *profils* actualisés en permanence, analysés et traités à *distance* des corps physiques, mais *pénétrés à flux tendus*, au sein de leur *équivalent numérique* – transparent et disponible. Masses de données conservées et soumises à des *dissections* portant sur des substances initialement organiques, sans fin redoublées sous forme de *magmas incorporels* de calculs électroniques en fusion.

La notion d'*avatar*, si souvent évoquée à l'occasion de l'usage de jeux en ligne ou de la navigation dans des environnements 3D, relève encore de la métaphore, dans la mesure où l'association opérée est forcée, par le fait de la

persistance d'un écart irréductible qui sépare le corps de sa supposée « copie ». La customisation d'un personnage dans *Second Life*, par exemple, ou dans d'autres « univers virtuels », ne correspond en aucune manière à l'engendrement d'une « créature dédoublée et autonome », mais à des *choix* dictés par une personne qui projette une conception d'elle-même sur une figure, formant ainsi une « trame numérique » « calquée » sur une conformation subjective et partielle. L'opération ne relève en rien de la « fécondation » d'un avatar, mais de l'élaboration d'une reproduction vague traitée par des robots électroniques, « autoportrait » réglé par des paramètres évolutifs et offert à la *représentation*. Or ce qui distingue l'avatar contemporain sous la forme discrète et sophistiquée des *bases de données*, c'est qu'il se soustrait de part en part à sa visibilité sur un plan, étant structuré par une matrice incorporelle multicritères irreprésentable mais seulement *quantifiable* par des *opérations imperceptibles* et *dynamiques* qui témoignent secrètement de la *profondeur de pénétration* à l'intérieur des corps et des consciences *en mouvement*.

On doit noter que l'extension des technologies numériques a tendance à produire un lexique souvent inadéquat, immédiatement accepté et répandu suivant des effets de généralisation hâtifs. Il s'opère soit des « retours du refoulé » à l'instar de la notion de « page » Internet par exemple, emblématique d'une modélisation fondée sur des structures déjà existantes, soit des *torsions nominatives* inappropriées, ce qui est exactement le cas dans l'emploi évoqué du vocable d'*avatar*, qui relève exactement dans ce cas-ci d'un abus de langage. Les bases de données, elles, « enfantent » précisément des avatars, dans le sens où des *répliques* de l'individu hypermoderne se « détachent » en continu de sa personne et vont se *loger* sous la forme de bits numériques sur des serveurs qui *hébergent* les « incarnations virtuelles » (virtualité ici entendue à la fois comme puissance toujours potentiellement à venir et comme processus immatériels qui autorisent des fouilles électroniques – simultanément opérées à distance des corps et *tout contre*).

Patrick McGoohan, le célèbre Numéro 6 de la série *Le Prisonnier*, répète en préambule de tous les épisodes : « Je ne veux pas me faire fiché, enregistrer, classer, déclasser ou numéroter. Ma vie m'appartient. » Au cours de chacune de ses tentatives d'évasion, une grosse boule blanche le rattrape implacablement et l'absorbe dans ses « entrailles », le ramenant toujours à sa localisation initiale. Dimension astreignante, manifeste et inflexible de la surveillance, aujourd'hui convertie en computations *indolores* qui visent uniquement à *évaluer* et à *devancer*. Ses modalités actuelles ne correspondent plus au régime de *contrôle* envisagé comme une procédure de *vérification* d'un certain ordre des choses (notre conception de la notion de « contrôle » demeure circonscrite à cette dimension d'*examen* de *conformité* aux classifications sociales et légales établies), or ce schéma ne recoupe plus les mécanismes déployés par la *surveillance contemporaine robotisée*, dont l'axe

majeur consiste à récolter des données, non pas en vue d'observer si les bornes sont respectées, mais dans l'objectif d'*analyser* les comportements, de les *mesurer*, de *projeter* des hypothèses d'action, en d'autres termes, d'instaurer une *intrusivité* historiquement inédite qui ambitionne prioritairement d'*anticiper* les *intentions* de malversation et les *désirs* d'achat.

Le traçage continu des personnes, la réduction de leurs actions à des calculs, interprétés et classifiés suivant des objectifs, ne relèvent pas du contrôle, entendu dans sa fonction historique d'examen structuré à l'égard du maintien d'une situation donnée, mais de la constitution à flux tendus de sommes de données analysables et exploitables en vue de pressentir les « desseins » des consciences. Contrairement à une forme historique de surveillance fondée sur l'exigence de répertorier l'attache familiale et professionnelle des individus, d'envisager chaque citoyen circonscrit à un espace délimité et affecté (domicile, lieu de travail), il s'est désormais dressé un *observatoire nomade* multipostes et multifonctions. D'une volonté de maîtriser un champ clos, borné à un cadastre à rotation lente (qui permit, par exemple, une gestion à la fois administrative et sanitaire de la peste à Venise, décrite par Foucault dans *Surveiller et punir*), un glissement s'est produit vers la généralisation d'une *capacité technique* à saisir les *mouvements* et *intentions* des corps. Une conception maintenant désuète supposait l'individu plus ou moins cantonné à une zone propre et à un registre d'activités limité (emblématique dans le modèle jacobin qui commande de quadriller le territoire par les préfets chargés de « faire remonter » les informations vers le pouvoir central), conformément à une politique du contrôle établie sur le signalement *centralisé* de troubles *localisés* avérés ou à venir⁴.

Or le véritable renversement produit par la surveillance contemporaine robotisée et géolocalisée regarde le fait singulier qu'elle se « nourrit » de la mobilité des personnes et de la volatilité de leurs comportements, qu'elle se bâtit d'après les déplacements, achats, communications, produisant d'autant plus de données utilisables qu'ils sont libres et fréquents. La plus grande indépendance d'action renvoie à la plus grande possibilité d'observation et d'analyse (le contraire exact du contrôle historique basé sur la nécessité de soumettre le corps à des restrictions réglementaires ou textes coercitifs). Dans le film *Ennemi d'État*, Gene Hackman (ancien de la NSA) explique au cours d'une conversation avec Will Smith (avocat pris dans un imbroglio qui l'oblige à fuir les membres de l'agence de renseignement), que « plus tu es branché technologies plus il est facile de te fichier ». Plus on voyage ou achète (selon les libertés fondamentales du droit à la circulation des personnes et des biens), plus s'amassent des volumes de données évaluables. La plus grande liberté est la condition paradoxale et contemporaine de la plus grande surveillance.

Machines désirantes

Les instruments de récolte des informations (robots fureteurs, capteurs, appareils biométriques, terminaux de paiements physiques ou virtuels) représentent d'une certaine façon, pour reprendre encore un concept fameux de Deleuze et Guattari, des « machines désirantes », dans la mesure où quantité de dispositifs sont « érigés » en vue de se rapprocher des corps, en quelque sorte de se fondre en eux, de satisfaire la « pulsion libidinale » des organismes sécuritaires ou des agences de marketing à vouloir gagner l'*intimité* d'autrui, à en jouir le plus intensément à la fois pour un orgasme de type masculin qui vise à *infiltrer* l'autre de sa propre semence, à lui implanter des *marqueurs* qui vont les lier – techniquement et parfois légalement (par exemple dans le cas de biopuces ou de bracelets électroniques destinés aux prisonniers « libérés » des murs physiques de la prison) –, et pour une extase de type féminin par l'absorption du sperme, cristallisation d'un désir achevé (achat, voyage...), capable de germer au contact des algorithmes chargés de le faire fructifier.

La métaphore sexuelle vise ici à exposer à quel point la *puissance de pénétration* des dispositifs de captation est rendue possible par un rapport toujours plus étroit entretenu au corps (dimension emblématique, nous le verrons, concernant les technologies biométriques), jusqu'à pouvoir bientôt suivre ses moindres oscillations (puces intégrées aux organismes pour une évaluation à flux tendus des flux biotiques et mise en place de protocoles d'alerte reliés à des unités médicales ou autres). Elle vise encore à signaler les principes d'entrelacement, de « fusion », qui s'opèrent entre machines et individus par incorporation de processeurs électroniques dans les veines, ou suivant les procédures à venir de « nano-implantation » encouragées par le développement des nanobiotechnologies. Enfin, elle souligne l'importance du *désir* à l'intérieur de cette architecture, celui éprouvé par chacun à vouloir vivre, voyager, acheter, librement : attiré pour les virtualités de notre présent, qui se fait inévitablement piéger ici ou là par les machines désirantes et sans retenue, qui prolifèrent sans fin dans l'environnement technique et social de ce début du XXI^e siècle.

Les bases de données, elles, ne relèvent pas de machines désirantes, mais sont notamment destinées à évaluer les *intentions désirantes* (ou malveillantes), dans l'objectif de *déduire* les desseins et non plus de constater les faits. La surveillance contemporaine sous la forme de collectes ininterrompues d'informations recueillies *auprès* des individus renvoie à une stratégie de *mesure* et non plus de vérification, d'*anticipation* et non plus de concordance. Pas un seul algorithme n'est aujourd'hui conçu en vue de savoir si telle personne respecte ou non la loi, mais ils sont tous tendanciellement configurés en vue de repérer des « postures déviantes » (qui peuvent cependant être tout à fait légales), entendues comme des comportements jugés décalés ou inappropriés, manifestes dans l'espace public ou tout autant dans le cadre de la vie privée (généralement « observée » sous la forme principale

d'interception de communications ou de transactions), et qui doivent être analysées et estimées en vue d'éventuellement intervenir *avant* la réalisation possible d'une entreprise menaçante.

La stratégie prioritaire mise en place, aussi bien par les organismes sécuritaires que par les unités de recherche en marketing, consiste à procéder par *recoupement*, à relever à la fois la *multiplicité* des pratiques qui composent l'environnement de chaque individu, et à établir son *réseau* de relations (elles-mêmes soumises à des examens identiques et à la consignation des antécédents, du milieu social, de l'origine ethnique...), de façon à pouvoir dresser une cartographie dynamique *individualisée et globale* du quotidien du plus grand nombre de femmes et d'hommes de la planète. Des agents de la NSA, dans le film *Ennemi d'État*, analysent simultanément les « *données comparatives* » entre deux profils, qui révèlent quantité de « jonctions » : retraits bancaires pour l'un, presque aussitôt suivis d'opérations de crédit de sommes identiques sur le compte de l'autre. Procédures d'observation « multicibles », capables de divulguer les proximités discrètes ou secrètes entre personnes, d'après un mode de perception des corps qui superpose sans cesse autopsie des multitudes singulières et estimation de leurs degrés d'affinité.

Ce gigantesque rhizome se forme grâce à l'infinité des *liens* qui unissent les êtres entre eux et les êtres aux choses, qui permettent de déduire des « significations » d'après des calculs élaborés sur des critères comportementaux, des modèles de proximité sociale, des calculs statistiques. Chaque personne est le point de départ et d'arrivée d'une immense toile *quantifiée* et tramée en continu grâce aux techniques qui explorent la structure et la *nature* des liens : le *link analysis*. Ces technologies ont été prioritairement développées depuis le 11 septembre 2001, suite aux défaillances des systèmes de renseignement qui n'ont pas su conclure à la préparation d'attentats, alors que la mise en *corrélation* entre de nombreux paramètres et similitudes aurait dû *alerter* (cours suivis et communs de pilotage, communications avec le Moyen-Orient, trains de vie supposés modestes et achats de sièges en classe affaires...). Une nouvelle logique axée sur l'impératif, sécuritaire et économique, d'anticipation, de *précognition* – avons-nous déjà dit à propos de la « vidéosurveillance intelligente », en référence au livre de Philip K. Dick et au film de Steven Spielberg *Minority Report* – s'instaure, se généralise et se perfectionne sans cesse, situant la notion même de contrôle en tant que procédure de vérification (la fonction des « télécrans » dans l'ouvrage d'Orwell, 1984) comme une catégorie historique définitivement obsolète.

La surveillance du XX^e siècle se chargeait de placer *sous contrôle* les personnes avérées délictueuses ou ennemies, ou s'intéressait particulièrement à celles susceptibles d'être suspectes ; la matrice du XXI^e siècle, elle, se déploie sur une estimation *indifférenciée* de la totalité des *unités* mobiles et

interconnectées, dont les gestes (communications et activités) vont produire des masses de données aptes à *signaler* des profils vers lesquels il faudra resserrer davantage le focus, non par une amplification des procédures d'observation, mais par la plus grande récolte informationnelle – en vue d'élargir le *spectre* des personnes éventuellement rattachées à l'unité initiale repérée et peut-être également en cause –, et arrêter une juste décision relativement au moment jugé opportun pour une intervention (une opération trop précoce, et c'est l'hypothèse de quantité d'informations précieuses qui seraient probablement perdues ; une initiative trop tardive, et l'acte serait déjà commis). C'est cette délicate tension que les agences de renseignement britanniques ont parfaitement maîtrisée en juillet 2006, dans le cadre du repérage de projets d'attentats simultanés sur des avions en plein ciel entre les États-Unis et l'Angleterre, qui leur ont permis de « remonter » de nombreuses connexions locales et internationales et de juger pertinemment du jour où procéder aux arrestations *avant* la réalisation des actes.

Un renversement historique s'est définitivement opéré : la consolidation des régimes démocratiques en Europe au début du XX^e siècle, fondée sur l'égal responsabilité des citoyens, ambitionnait seulement de *suivre* les fautifs probables, et veillait en même temps au respect des bornes légales, à l'aide d'appareillages multiples (présence policière, consignation des antécédents judiciaires, examen de la conformité aux registres civils, expertise de la santé mentale par la médecine du travail ou les organes sociaux...). Suivant une logique qui visait non pas un retrait des forces de sécurité mais à réprimer uniquement tout fait ou événement susceptible de troubler l'ordre public. Bien sûr, le *renseignement* correspond à une pratique bien ancienne – autrement nommé « le deuxième plus vieux métier du monde » –, grâce auquel un personnage comme Vidocq, au XIX^e siècle, a pu établir l'efficacité et la puissance de sa police parisienne, à l'aide de son réseau d'indicateurs, la plupart recrutés au sein de la pègre, qu'il s'agissait d'*infiltrer*. Mais ces manœuvres qui ponctuent une longue généalogie – poursuivie à peu près jusqu'à la chute du mur de Berlin en 1989 – se déterminaient toujours en fonction de *milieux* déjà identifiés, devant faire l'objet d'une « attention » particulière (par exemple, les groupes de « guérillas gauchistes » durant les années soixante-dix en France, en Allemagne, en Italie : Action directe, Bande à Baader, Brigades rouges...).

Certes, ces principes de « focalisation » persistent (surveillance particulière déployée à l'égard des « réseaux islamistes » aux États-Unis, en Grande-Bretagne, en France, en Allemagne, aux Pays-Bas...), mais ils ne représentent plus qu'une « stratégie additionnelle » à la nouvelle machine de guerre interconnectée et géolocalisée, qui instaure une *mesure d'évaluation commune* visant à collecter la plus grande quantité d'informations à partir du *profilage* (sécuritaire et marketing) de la *totalité* des êtres vivants. Le « cœur » de la méthodologie élaborée par la surveillance du début du XXI^e siècle

consiste à opérer suivant une *indifférenciation généralisée des cibles*, à soumettre la planète entière à un *moissonnage globalisé* de données, de façon à ce qu'au moyen d'algorithmes adéquats et de processeurs computationnels toujours plus puissants il se dégage des cartographies dessinant automatiquement des trames hyperindividualisées, appelées à faire l'objet de *traitements* appropriés et dynamiques, selon les *circonstances politiques* ou les *offres commerciales*.

Changement de paradigme

Cette « hypersurveillance » trouve actuellement les conditions idéales de son épanouissement et de son perfectionnement, par le simple fait qu'elle se déploie au sein du « bouillon de culture » contemporain déjà évoqué, qui *mêle* trois ingrédients somme toute récents, majeurs et décisifs : *dispositifs techniques numériques* (interconnexion, géolocalisation, biométrie...) ; *incertitude terroriste* (positionnements atomisés et virtualité permanente du risque qui pousse non plus au « contrôle » de l'ennemi mais à sa *détection*, et à la *déduction* de ses intentions selon un ordre *anticipatoire*) ; *marketing*, qui ne cherche pas seulement à vérifier qui a acheté quoi, mais à établir des tableaux comportementaux personnalisés en vue de *projeter* les désirs d'achats conscients et inconscients, de les devancer, de les susciter, et plus encore de pouvoir les *combiner* à d'autres, d'élargir toujours davantage l'horizon des aspirations... L'entrelacement progressif entre ces différents paramètres renvoie au « problème des trois corps » de Poincaré, qui établit que l'enchaînement des effets à partir de l'apparition d'un troisième terme interdit toute prédiction possible par le fait d'équations sans cesse différentielles, impossibles à fixer une fois pour toutes. Les interactions entre trois données distinctes dissolvent *de facto* les « intégrales premières », c'est-à-dire les fonctions recouvrant une valeur constante qui échappent, dans leur interférence complexe, au calcul. Probablement sommes-nous et serons-nous encore davantage confrontés à ce régime de surveillance de nature *systémique* imprédictible et échappant sans fin et en partie à des procédures concertées de régulation, suivant des vitesses de déchaînement de nature organique, qui devront être *orientées* d'après une vigilance soutenue par chaque individu autonome et responsable et chaque organe d'intérêt public ou État démocratique soucieux de veiller aux libertés fondamentales, tenues jusque-là pour absolument irréductibles, et maintenant soumises à la violence de ces « électrochocs » en fusion.

Il est possible d'affirmer qu'une rupture décisive s'est produite : l'instauration d'un nouveau paradigme technologique et anthropologique qui entraîne avec lui un modèle historiquement inédit de surveillance, à l'intérieur d'un environnement global non plus caractérisé par des « sociétés de contrôle » (terme obsolète formé sur la *vérification* et la *conformité*). La formule de Deleuze date d'une époque finalement récente (1990)⁵, dont on

voit qu'elle appartient à une *épistémè* dépassée et qu'à la fois elle cristallisait une sorte d'achèvement technologique qui permettait à quantité de dispositifs de quadriller les espaces physiques à l'aide de moyens électroniques élaborés, mais à la *multiplicité des fonctionnalités* réduite, et prioritairement affectés à assurer un *ordre conforme*. La courte distance temporelle qui nous sépare de cette phase signale la précipitation et la nature du glissement opéré, qui modifie une ère principalement soucieuse du maintien d'une tension moderne entre droit et sécurité, vers la *génération* d'une *matrice hypermoderne et globale*, qui vise sans frein et en tous points à *implémenter* la planète de programmes ultrasophistiqués de *pénétration universelle des consciences*.

La fonction cruciale assurée par les récoltes et stockages informationnels induit un processus de *dématérialisation* de l'armature générale de la surveillance. Non seulement la dimension de suivi physique des corps renvoie à une modalité quasi révolue, mais les dispositifs qui restent visibles (cependant appelés à être toujours plus « fondus » aux surfaces matérielles) ne constituent plus que des « témoins » encore percevables destinés à « alimenter » les processeurs électroniques. Les bases de données représentent des « vampires contemporains » qui ne cessent de « sucer notre sang », qui « absorbent » la *substance vitale* de leurs victimes, pas seulement durant des nuits d'épouvante mais sans discontinuer dans le temps, et qui, à l'instar de leurs ancêtres fantasmatiques, agissent par surprise ou plus précisément de façon insidieuse, ou tétanisent tout effet de lucidité consciente dans le cours de notre quotidienneté (achats par carte bancaire, par exemple) par le fait qu'elles revêtent l'extrême particularité de n'apparaître jamais comme telles, puisqu'elles sont proprement *invisibles*. Elles se présentent parfois sous des contours ostensibles (moteurs de recherche, comptes bancaires, annuaires téléphoniques), mais leur constitution, sous la forme de captation des flux, de calculs et d'analyses, demeure de part en part soustraite à la perception sensible. Cette dimension de *transparence* leur assigne une condition « en retrait », une forme mystérieuse qui confirme leur implacable puissance, offrant l'avantage de les protéger tendanciellement de la protestation, et ce alors qu'elles représentent le « cœur » de la surveillance contemporaine, qu'elles en sont en quelque sorte les « superstars ». À la différence de la vidéosurveillance, qui fait l'objet de toutes les contestations, cristallisées dans la vue manifeste des caméras qui cependant ne figurent qu'une forme maintenant mineure de la matrice, ou alors plus massive dans le cas de plus en plus fréquent où elles sont *articulées* aux banques de données, seulement dressées en vue de leur transmettre des images désormais réduites à des codes analysés, traités, ou combinés à d'autres types de datas.

Les techniques d'espionnage – nécessairement furtives – ont toujours revêtu au cours des âges une forme de *matérialité* susceptible de les rendre finalement repérables (jumelles, micros, caméras...). *Brazil*, le film de Terry Gilliam, expose une société entièrement structurée par une

« hyperbureaucratie », ponctuée de part en part par quantité d'écrans (dont la fonction et l'allure désuète font penser aux « télécrans » de 1984 d'Orwell – *partout ostensibles*), et par un usage inflationniste d'imprimés et de formulaires de toute sorte qui constituent les archives *manifestes*, relatives aux identités et aux gestes des personnes. Sommes d'informations produites selon une telle densité qu'elles saturent *physiquement* les espaces de travail des services concernés, à l'opposé des calculs générés par les bases de données, « sauvegardés » sur des disques durs qui structurellement déjouent la dimension même de « vision ». À moins d'être médiatisées par des interfaces, mais leur particularité réside encore dans le fait que leur visibilité sur des écrans ne constitue que des résultats *partiels*, issus de requêtes précises, et qu'aucun schéma ne pourra jamais *entièrement* rendre compte des « magmas computationnels » qui s'opèrent sans fin d'après les traces disséminées par chacun. Une part secrète (« maudite » ?) et irréductible caractérise inévitablement ces nouveaux « monstres » ou « fantômes contemporains » *incorporels*, en quelque sorte « inexistants », s'agrégeant cependant toujours davantage à nos décisions et actions quotidiennes.

De surcroît, comme pour renforcer dans les faits autant que symboliquement leur « aura impénétrable », ces informations sont généralement situées sur des serveurs disposés à l'intérieur de pièces stérilisées qui en défendent l'entrée, exception faite à des techniciens spécialisés. Vision interdite de ces « batteries mémorielles exosomatiques », gardées et entretenues avec presque autant d'attention et de *paranoïa* que des ogives nucléaires. Opacité radicale qui rend presque impossible l'hypothèse de leur « mise à plat » en vue d'une plus grande « clarté » des processus et des usages, et qui leur octroie une position « à l'écart », presque inabordable, formalisée par un processus apparemment contradictoire : elles infiltrent suivant des courbes exponentielles notre environnement contemporain, et *simultanément* fuient sans fin vers un « ailleurs » inaccessible. Pour la première fois dans l'histoire, un système de récolte et de conservation d'informations prises sur les individus recouvre une forme insaisissable, d'autant plus paradoxale qu'il innerve profondément notre quotidien. À la fois *omniprésent* et absolument *invisible*.

« Bentham a posé le principe que le pouvoir devait être visible et invérifiable⁶. » Cependant, à la différence de la fin du XVIII^e siècle, mais également de l'époque durant laquelle Foucault analysait la nature des organes de discipline et de contrôle, nous n'avons désormais plus affaire au « pouvoir » en tant que figure singulière, homogène et coercitive, mais à quantité de faisceaux et de nœuds plus ou moins puissants (politiques, économiques, médiatiques, associatifs...) qui interdisent *de facto* la détermination close d'une autorité unique et surplombante. Alpha 60, calculateur quasi omniscient, règle d'après ce principe pyramidal la bonne conduite d'Alphaville (Jean-Luc Godard, *Alphaville*, 1965) ; la machine

représente une forme automatisée et transcendante du contrôle dans un environnement hautement technicisé, conduisant « naturellement » à un devenir autoritaire des sociétés (suivant une vulgate très répandue au cours des années soixante). La structuration des bases de données contemporaines, elle, ne renvoie pas à une architecture unitaire et indivisible, mais à quantité de masses *éparses* aux fonctionnalités multiples, qui confirment l'extrême *atomisation* des instances et lieux d'influence, évoquée au cours de notre introduction. Elles accompagnent et favorisent à la fois ces jeux de dissolution des ordres hiérarchisés dans la mesure où elles ne sont pas (encore) gérées par des organismes centralisés, mais forment une *myriade* de constellations plus ou moins éclatées, *enfouies* et *immatérielles*.

D'une certaine façon, elles tétanisent l'illusion d'un régime omnipotent et contribuent à défaire des schémas binaires, situant d'un côté la souveraineté et de l'autre les sujets, d'après des schémas conceptuels à l'œuvre depuis la Révolution française. Elles opèrent un double mouvement concomitant qui recouvre encore une dimension anthropologique : foisonnement ininterrompu de flux logés sur des « serveurs » (autre nom possible des formes contemporaines – plurielles – de « pouvoirs ») et disparition des processus sensibles d'intimidation par le fait de leur *incorporalité*. Enfin, leur puissance de pénétration toujours plus intrusive ne rend pas leur réalité *invérifiable*, c'est même tout le contraire puisqu'il n'est pas une opération transmise ou reçue par les objets interconnectés (alertes SMS, fils RSS, recherche d'informations sur Internet...), qui ne confirme leur efficacité et leur « pertinence » constamment *vérifiables* et achèvent ainsi de renverser mot à mot ou point par point la formule de Foucault citée plus haut, comme un témoignage implacable du surgissement définitif d'une nouvelle *épistémè*, marquée par l'*intensification* des *liens* entre les *terminaux* organiques et électroniques.

Totale asymétrie

Qui peut prétendre demander à « voir » les bases de données ? La revendication paraît absurde. Une fois encore, la nécessaire parade à ces processus de pénétration radicale et invisible consisterait à dresser des lois en vue de fixer des bornes. Situation complexe, nous l'avons vu, dans la mesure où la circulation des flux électroniques ignore les frontières et les cadres légaux nationaux (certains États, par exemple, proscrivent la pratique du « spam » ou des « agrégations » plus ou moins étendues de données provenant de sources hétérogènes). Néanmoins, il semble manifeste qu'un mouvement en quelque sorte « parallèle » se met en place, qui en partie respecte les restrictions juridiques, et qui d'un autre côté est « absorbé » par les virtualités technologiques et l'extrême facilité à capter ici et là les traces disséminées. Un équilibre fragile et incertain caractérise les mécanismes de saisies informationnelles, nécessairement appelés à se plier aux règlements et

toujours disposés à capitaliser la puissance des systèmes, dont les procédés, nous l'avons dit, échappent à la perception sensible. Faut-il considérer qu'il est déjà trop tard pour tenter de ralentir ou de retenir cette nouvelle intrusivité universelle ?

Organes sécuritaires et bureaux de marketing ne cessent de perfectionner leurs « machines de guerre » suivant des configurations appelées à se perfectionner et à s'affiner sans cesse, sans que législateurs ou citoyens n'aient véritablement pris la mesure abyssale de la nature et de la portée des infiltrations généralisées qui prolifèrent *en silence*. Une tension *asymétrique* s'instaure qui repousse la possibilité de la contrecarrer par le fait de la disparition de la « relation frontale » (qui caractérise particulièrement la vidéosurveillance : le corps *face* à des caméras), et qui autoriserait des jeux de *confrontation* dialectique et critique, ou la mise en place de « rapports de force » salutaires, destinés à placer les dispositifs sous une vigilance continue. Fritz Lang ne montre jamais le docteur Mabuse ; les personnes à son service ne distinguent qu'un rideau fermé et perçoivent seulement une voix, qui confirme par son absence corporelle son pouvoir absolu, quasi divin⁷. L'« enveloppement incorporel » par des fantômes qui accompagnent notre quotidien empêche dans les faits de se dérober, à moins de refuser l'usage du téléphone, d'Internet, de cartes bancaires, de ne pas se déplacer (néanmoins demeurerait encore les dossiers médicaux, les documents d'identité...). Impossible de se soustraire aux « vampires numériques », ou il faudrait se retirer absolument du monde ; ambition probablement insuffisante car la vie contemporaine, où que l'on soit et malgré nous, sous une forme ou une autre, génère désormais quantité de données.

« À la lourdeur des vieilles “maisons de sûreté”, avec leur architecture de forteresse, on peut substituer la géométrie simple et économique d'une “maison de certitude”. [...] Le pouvoir externe, lui, peut s'alléger de ses pesanteurs physiques ; il tend à l'incorporel ; et plus il se rapproche de cette limite, plus ses effets sont constants, profonds, acquis une fois pour toutes, incessamment reconduits : perpétuelle victoire qui évite tout affrontement physique et qui est toujours jouée d'avance⁸. » Les analyses développées par Michel Foucault dans *Surveiller et punir* témoignent de la portée des évolutions qui ont transformé les systèmes de contrôle, et ce non seulement depuis le siècle de Bentham mais tout autant depuis la période durant laquelle Foucault rédigeait son ouvrage, qui constitue au sein de notre enquête un « marqueur temporel » qui *signale* la nature des glissements qui se sont opérés depuis le XVIII^e siècle tout autant que depuis le deuxième tiers du XX^e siècle, et qui ont profondément modifié l'économie générale de la surveillance. Si le *Panopticon* cristallisait une nouvelle forme d'observation des individus qui allait se prolonger longtemps après, par effet de persistance structurelle sous des formes diverses, nous sommes ici contraints de pointer les phénomènes de *rupture*, les mutations radicales qui se sont déployées par le fait de

l'avènement conjoint de plusieurs facteurs techniques, économiques et géopolitiques, qui composent ce « bouillon de culture » inédit, dont les effets passés ont déjà contribué à renverser en un intervalle temporel somme toute très réduit des ordres historiques profondément enracinés. Les processus à l'œuvre dans les bases de données dessinent bien davantage qu'une seule ruse architecturale destinée à instaurer un autre type de rapport au prisonnier, elles imposent désormais une nouvelle « couche » au sein de notre quotidienneté, qui enveloppe *tout* individu et dissout la figure binaire *opposant* « regardeur » et « regardé » au profit de « pompes aspirantes » omniprésentes, « softs » et insensibles.

Un *saut* s'est produit, qui abandonne la nécessité historique de placer sous *contrôle* des individus ou groupes potentiellement menaçants par effet de focalisation précisément orientée et ciblée, vers une *réduction* systématique et *indifférenciée* des corps et des comportements à des masses de calculs analysées et traitées, en vue d'usages non plus exclusivement d'ordre *sécuritaire* mais dorénavant tout autant *commercial*. Bond d'une même puissance (ou violence) que celui du retournement du régime de la vérification et de la conformation vers la nouvelle exigence de *précognition* généralisée des actes et des désirs. Franchissement technologique et anthropologique de deux *seuils* indissociables, l'un de nature horizontale, l'autre de nature verticale : le premier cherche à *universaliser* ses processus, le second ambitionne de *pénétrer* toujours plus profondément les consciences. Instauration d'une « hyperévaluation » de masse, non pas réglée par des instances surplombantes et unifiées mais par des organes de captation disséminés aux objectifs hétérogènes, qui n'aspirent pas à vérifier mais à *cartographier* en vue de l'élaboration de stratégies sécuritaires ou marketing mobiles et évolutives, hautement ajustées et individualisées. La récolte contemporaine de traces s'accroît suivant des courbes exponentielles, et d'après des puissances de transmission, d'analyse et de stockage qui renvoient à la fameuse loi de Moore établissant le doublement des performances techniques tous les dix-huit mois. D'une certaine façon, cette équation pourrait revêtir encore une valeur symbolique, celle qui confirmerait l'intensification continue d'une « hyperinfiltration globale », d'ores et déjà tendue vers des processus aux mesures *nanométriques* et *quantiques*.

Il se dessine les prémices d'un « âge d'or » des bases de données, qui profitent de conditions multifactorielles appelées à consolider leur position pivot dans le champ social et économique et à perfectionner sans fin leurs modalités et finalités d'usage. « L'ordinateur est à la vie privée ce que la mitrailleuse était à la cavalerie », avaient affirmé en 1978 le juriste américain Alan W. Schefflin et le chercheur en psychologie Edward M. Opton Jr., dans leur livre rédigé en commun *The Mind Manipulators*⁹. Cependant, aujourd'hui, ce n'est plus l'ordinateur qui représente le dispositif central de dissémination de données, mais le *foisonnement* d'instruments électroniques de réception et de transmission d'informations qui témoignent *en chœur* du

rythme de nos existences. Ils nous encouragent à prolonger la métaphore d'ordre militaire, en affirmant que si un équipement plus ou moins isolé pouvait recouvrir la valeur d'une « mitrailleuse », la multiplicité de protocoles *interconnectés* et *géolocalisés* (intégrés aux corps ou aux objets), infiltrant sans fin notre quotidienneté, augure selon une probabilité quasi certaine un avenir proche tramé par quantité d'« armes de pénétration massives » – d'aspect ludique et aux fonctions pratiques –, néanmoins aptes à annihiler le droit historique garantissant la vie privée¹⁰. L'individu contemporain s'expose désormais comme une cible sécuritaire ou commerciale précisément identifiée et continuellement *profilée*, par le fait de la production à flux tendus de diagrammes évolutifs qui tendent vers un but ultime : soumettre les êtres à une *transparence totale* par le *redoublement* exact des corps et des consciences en des masses de données, actualisées en temps réel à la vie ou à l'*intimité* de chacun.

Classifications « verticales »

Une partie de l'architecture des bases de données se compose de *fichiers spécialisés* qui regroupent des renseignements à la classification très spécifiée dont la mise à jour s'opère par introduction exclusive de nouvelles informations de même nature. Ils relèvent le plus souvent d'instances étatiques (ministères de l'Intérieur ou de la Défense ; Sécurité sociale ; services fiscaux...), et correspondent à des modes de recensement bien anciens, aujourd'hui facilités par les technologies interconnectées, sous la forme d'un accès, d'une visibilité et d'une capacité de mise en relation infiniment plus aisés. Au cours des deux premiers tiers du XX^e siècle, leur emploi s'est rationalisé (notamment par l'apparition de l'informatique à partir de la fin des années cinquante), mais ils n'ont pas connu une amplification notoire de leur nombre, suivant une nature de registres demeurée tendanciuellement similaire au cours de cette période. En revanche, le dernier tiers du XX^e siècle aura vu une expansion des procédures de fichage. En France, par exemple, la quantité de fichiers de police et de gendarmerie s'est considérablement accrue depuis le milieu des années quatre-vingt-dix – souvent sans concertation préalable avec les différentes parties susceptibles d'être concernées –, au point de susciter des réclamations relatives aux conditions juridiques de leur utilisation, ou des interrogations d'ordre plus pratique concernant leur interopérabilité et la véritable efficacité d'un tel foisonnement.

Une commission mise en place par le ministère de l'Intérieur en 2006, présidée par Alain Bauer entouré de compétences multiples (responsables de police, de gendarmerie, juristes, président de la CNIL, journalistes...) pointe, dans son rapport¹¹, trois écueils principaux : celui de l'actualisation des fichiers estimée lente et incomplète (particulièrement celle de la suppression des noms demandée par la Justice) ; celui de la difficulté de vérification par

les citoyens, généralement mal informés ; enfin celui des conditions de leur utilisation dans le cadre d'enquêtes administratives. L'ensemble de ces complications « fait apparaître un certain nombre de dysfonctionnements », notamment par le fait d'un usage privilégié accordé aux forces de l'ordre, au détriment d'une même condition d'accès permise aux instances juridiques, cependant appelées à contrôler le recensement de leur décision dans la mise à jour des données (par exemple certains non-lieux n'auraient pas été systématiquement suivis d'annulation dans les index). L'instauration en France du « dossier médical personnalisé » (DMP) va encore contribuer à regrouper des volumes de renseignements spécifiques sur les personnes, certes suivant des objectifs peut-être bénéfiques, consistant à connaître le plus rapidement les antécédents médicaux des patients (à l'attention des hôpitaux et médecins) – exposant ainsi chacun à une nouvelle *radiographie* « mnémotherapeutique » *consultable* –, mais dont on ne sait pas très bien encore dans quelles conditions de confidentialité, notamment à l'égard des compagnies d'assurances et des employeurs, ils seront employés techniquement et légalement. Le fichier national automatisé des empreintes génétiques (FNAEG), initialement destiné à répertorier exclusivement les délinquants sexuels, archive maintenant la quasi-totalité des crimes et délits sous forme d'identifiants ADN, confirmant à quel point puissance technologique et relative indifférence des citoyens favorisent non seulement l'expansion de la pratique de la classification systématisée des infractions, mais surtout leur mémorisation d'après des durées souvent aléatoires.

La généralisation du fichage des individus produit dans ce cas-ci non des cartographies globales mais une sorte de *division* toujours plus fine et *distribuée* des corps et des comportements, à l'intérieur de segments *spécifiques* qui découvrent une nouvelle *profondeur* dont l'efficacité provient ici d'une compartimentation « hyperverticale » des données. Le recoupement croissant entre profils hyperspécialisés et autres sources offre une nouvelle puissance de visibilité des antécédents que certains voudraient pérenniser sous la forme standardisée de l'*interopérabilité*. Protocole qui consiste à relier systématiquement différents registres (particulièrement ceux de police), en vue d'accroître la rapidité et l'efficacité des enquêtes. La dispersion des services et de leurs renseignements nécessite d'instaurer des procédures d'interconnexion aptes à favoriser des opérations en réseau et à lancer des *alertes multicritères*. L'objectif vise la consultation mutuelle des informations établies par chaque unité grâce à un *accès partagé*. Néanmoins, ces mécanismes régis par des instances étatiques témoignent d'un régime sécuritaire en quelque sorte situé « à la traîne » des modalités contemporaines et hypersophistiquées de cartographies des singularités – étant gérés par *recouvrements dynamiques* continuellement *modulés* en temps réel. L'avant-garde de la récolte de données est aujourd'hui conçue et programmée par le *marketing contemporain* qui fonde le socle de sa stratégie du début du

XXI^e siècle sur une extrême *individualisation* des profils, rendue possible grâce à la collecte et à l'analyse à flux tendus des *traces numériques* diffusées par *chaque* consommateur *unique*.

Sophistications marketing

Depuis le début des années quatre-vingt, la « science des marchés » a connu une rapide évolution de ses méthodes, fondées alors sur des principes d'identification en différentes « tranches » (âges, catégories sociales et professionnelles, localisations...). Ensuite, durant la décennie suivante, l'amplification des phénomènes concurrentiels suivant une échelle désormais globale a conduit à affiner les techniques, à abandonner les groupements génériques, jugés trop massifs, au profit de la conception de « segments » capables de prendre en compte les phénomènes de « multi-appartenance¹² » et de disséquer des « cibles » toujours plus volatiles d'après des grilles « multicritères¹³ ». L'augmentation continue des volumes de stockage numérique associée à l'affinement des traitements informationnels a favorisé l'instauration de bases de données commerciales, capables de *différencier* et de *détailler* ces nouvelles « niches » de populations. L'enjeu majeur consistant à établir une relation suivie avec *chaque* individu, de façon à pénétrer les conduites de consommation et à définir un portrait exhaustif (habitudes, pouvoir d'achat, psychologie...) apte à informer les algorithmes destinés à proposer offres adaptées ou à devancer les désirs encore enfouis¹⁴...

À l'amorce du nouveau millénaire, l'interconnexion généralisée (Internet, paiements électroniques par cartes bancaires et de fidélité, numérisation d'opérations de toutes sortes...) a permis une *traçabilité individualisée* et continue des comportements qui génère des « océans exponentiels de données », stockés, analysés, et traités dans l'intention d'intensifier une « relation personnalisée au client ». Le marketing a su conjointement profiter de la puissance informatique et du constat postmoderne de l'absolue singularité de chaque être, pour capitaliser cet acquis philosophique et social sous la forme d'un observatoire robotisé des conduites, tendanciellement dressé en vue de *pénétrer les consciences*. Une discipline initialement chargée de concevoir des techniques systématisées de vente s'est progressivement transformée en machine planétaire de suivi, programmée à connaître les *préférences* de chaque « terminal humain » et à établir un lien d'intérêt mutuel singularisé et ininterrompu. Gilles Deleuze écrivait déjà en 1990 – alors que les éléments de l'interconnexion généralisée se mettaient seulement en place et qu'elle a depuis enveloppé la planète, donc infiniment accru la sophistication des méthodes de quantification des individus : « Le marketing est maintenant l'instrument du contrôle social, et forme la race impudente de nos maîtres. Le contrôle est à court terme et à rotation rapide, mais aussi continu et illimité, tandis que la discipline était de longue durée, infinie et discontinue¹⁵. »

Les agences de communication ne constituent que très rarement leurs fichiers, mais font appel à des sociétés spécialisées dans l'établissement et le commerce de bases de données personnelles et comportementales ; activité en plein essor, propre au « secteur quaternaire » fondé sur les transactions dites « immatérielles », ou plus précisément de nature strictement informationnelle. La stratégie majeure vise à accumuler le plus grand nombre de renseignements à l'égard de chaque « prospect », à *ajuster* des profils extrêmement précis selon une technique privilégiée : soumission de questionnaires – parfois rémunérés, ou à l'occasion de l'affiliation à un programme de fidélisation, à l'inscription d'un site d'achat... – invitant à détailler profession, situation familiale, loisirs, habitudes alimentaires... De surcroît, ces « confessions intimes » contemporaines peuvent être *agrégées* aux achats effectués par cartes de crédit, aussi bien en magasin que sur Internet, permettant de dessiner des cartographies singularisées, à la fois stables (conditions générales d'existence) et évolutives (conduites de consommation quotidiennes)¹⁶.

Les navigations à travers les sites Web peuvent encore être archivées à l'aide d'un logiciel contenant un numéro d'identification (cookie) automatiquement infiltré sur le disque dur. DoubleClick – la plus importante société de publicité en ligne, récemment acquise par Google – organise notamment, à l'aide de cet outil, la distribution ciblée de bannières sur les pages. L'enjeu consiste à s'accorder le plus pertinemment aux usages de chaque internaute, en vue de faire apparaître des annonces *sur mesure*. La notion de « *rich media* » conceptualisée par l'entreprise définit l'étendue et la *profondeur* des possibilités relationnelles et commerciales que la connectivité autorise. Elle appelle la mise en place de stratégies ambivalentes, à la fois intrusives et propres à inspirer confiance ; c'est dans l'intention de maintenir autant que possible cet équilibre que les collectes informationnelles se constituent désormais avec l'assentiment exprès, selon le principe de l'« *opt-in* », qui suppose une implication consciente et autorise en théorie la désinscription.

La tension entre présence d'un individu à l'intérieur d'une zone géographique et propositions commerciales adaptées et situées à proximité constitue encore un axe majeur des recherches marketing. Google, par exemple, offre à San Francisco une connexion Wi-Fi gratuite en échange de quoi l'utilisateur accepte de recevoir des publicités ciblées en fonction de sa localisation. En France, l'INRIA a développé un partenariat avec la société JCDecaux, qui permet au groupe publicitaire d'utiliser les technologies d'« *informatique diffuse* ». L'opération nécessite le consentement de l'usager, qui aura préalablement enregistré indications et « préférences » (âge, activités, loisirs...), et sera physiquement identifié au moyen de son téléphone portable par les senseurs intégrés aux panneaux d'affichage. « Devant une publicité

pour un film, le passant pourra regarder la bande-annonce sur son portable, explique Albert Asseraf, directeur de la stratégie, du marketing et des études de JCDecaux. Devant une affiche de voitures en promotion, il recevra l'adresse du point de vente le plus proche par SMS, s'il est un passionné de voitures¹⁷ ».

Au Japon, les passants peuvent diriger l'œil de leur téléphone vers les codes-barres visibles sur des affiches, et sont mis en relation avec des sites Web fournissant indications complémentaires ou proposant des promotions à saisir dans les boutiques les plus proches. L'enjeu consiste à instaurer une *relation automatisée* entre objets de l'environnement (arrêts de bus, surfaces publicitaires, vitrines...) et prothèses numériques individuelles. Les tissus urbains sont appelés à être toujours plus infiltrés de capteurs destinés à « dialoguer » avec les citoyens, situant chacun comme une virtualité d'achat continue qu'il s'agira d'*orienter* le plus pertinemment en fonction de ses goûts et de ses diverses déambulations dans l'espace. Jean-Charles Decaux, codirecteur général de JCDecaux, précise : « Être un média de masse c'est bien, mais pouvoir personnaliser notre relation avec le consommateur, c'est la nouvelle frontière de l'affichage¹⁸. » La *tension dynamique* opérée entre corps et territoires correspond à une nouvelle faculté de type « horizontal », destinée à capitaliser quantité de renseignements stockés et traités de façon à favoriser la relation d'un point (le consommateur) à un autre (lieu de vente ou de service), à l'intérieur d'une *surface plane* qui autorise des *adéquations* spatiales et temporelles *ajustées*. Un autre objectif simultané ambitionne d'établir un *rapport vertical* au même consommateur à l'intérieur des profondeurs de sa psychologie, en vue de *prédire* – en quelque sorte avant lui – ses gestes et aspirations à venir.

Pénétrer l'esprit

La volonté de saisir les « intentions » exige un perfectionnement soutenu des modalités de *profiling*, par la plus grande *accumulation* de renseignements provenant de *sources éparses* et par la plus haute pertinence des analyses opérées. Une technique relativement récente autorise la réalisation de cette double exigence : le *data mining* ou « fouille de données ». Procédure qui permet de dégager des constantes significatives à partir de volumes informationnels qui, sans elle, seraient demeurées dissimulées. Le procédé ne suppose pas la formulation d'une hypothèse initiale qui appellerait ensuite sa vérification par le calcul ; ce sont les algorithmes eux-mêmes qui *révéleront* des corrélations *insoupçonnées*. Ils transforment en information le traitement de masses indifférenciées auparavant « silencieuses », suivant une méthode sans *a priori*, qui cherche à faire émerger à partir de volumes bruts des inférences jusque-là inconnues. La pratique a pu se développer grâce au croisement des sciences de la statistique et de l'intelligence artificielle. Une sorte d'origine plus ou moins avérée du *data mining* remonterait à la mise en

évidence par les magasins Wal-Mart d'une forte concordance entre achats de couches pour bébés et de bières les samedis après-midi. Les analystes comprirent que le phénomène était dû au fait que des hommes étaient souvent chargés ce jour-là par leurs compagnes de se rendre dans les magasins pour acheter les volumineux paquets. Les rayons furent réorganisés en conséquence, par une proximité entre les deux types d'articles dont les ventes augmentèrent de concert.

Le dispositif opère une inversion dans le rapport usuel aux données : pas de ciblage préalable mais l'obligation de ratisser le plus grand nombre possible d'indices *de tout ordre*. Renversement majeur qui pousse chaque individu, et malgré lui, à expliciter la nature des liens qu'il opère dans le temps, sans qu'il en ait pleinement conscience ; renseignements désormais divulgués par les conclusions algorithmiques. On comprend mieux en quoi la notion de « pénétration de l'âme » ne recouvre aucune exagération mais correspond exactement à la tendance la plus emblématique, à l'aspect « futuriste » et pourtant déjà bien réel, de la surveillance contemporaine. « Les trois opérateurs de téléphonie mobile français, Bouygues, Orange et SFR, estiment que les modèles comportementaux qu'ils ont élaborés grâce au *data mining* leur permettent de repérer à l'avance les clients susceptibles de passer à la concurrence ou ceux capables de souscrire des forfaits plus chers¹⁹. » On peut supposer que, de leur côté, ces mêmes clients ignorent encore leurs probables velléités, mais qu'ils les « portent » déjà en eux sous une forme plus ou moins inconsciente. Le *data mining* inaugure une nouvelle ère qui dépasse le concept de « *profiling* », entendu comme une classification individualisée des comportements et des préférences, vers celui d'une « intuition robotisée des motivations » qui vise, elle, à déchiffrer ce qui détermine la *corrélation* entre différentes décisions majeures ou mineures.

Les « precogs » de Philip K. Dick que nous avons évoqués trouvent aujourd'hui les conditions de leur avènement, non plus sous la forme hybride d'êtres de chair infiltrés de composants électroniques mais d'une architecture cybernétique hypersophistiquée rendue possible par l'intelligence artificielle, désormais capable de « comprendre » ce qui se joue de structurant le long des séquences ininterrompues qui forment les trames de nos décisions. « Le MIT affirme que le *data mining* constitue une des dix découvertes qui changeront le monde au cours du XXI^e siècle²⁰. » Une telle « puissance intrusive » ne pouvait évidemment pas être ignorée par les *intelligence agencies*, qui se sont vite emparées du procédé originellement conçu en vue d'approfondir la connaissance du consommateur. Événement qui confirme à quel point techniques de marketing et techniques sécuritaires sont entremêlées, se servant de leurs innovations mutuelles avec le même objectif : suivre les comportements *à la trace* en vue de *devancer*, pour les unes, les *désirs* d'achat, pour les autres, les *intentions* malveillantes. Plus encore, ce sont les récoltes relatives aux pratiques de consommation qui aujourd'hui nourrissent le renseignement contemporain, non plus chargé de pister les actions illégales

mais tendu vers la *compréhension intime* de la vie quotidienne du plus grand nombre d'habitants de la planète : « Selon Jeffrey Ullman, l'examen minutieux des bases de données commerciales permettra bientôt de repérer des transactions suspectes, signe qu'Al-Qaïda prépare une opération²¹. »

Une partie des recherches publicitaires contemporaines vise une étape ultérieure : la compréhension des schémas cérébraux sous le vocable significatif de *neuromarketing*. L'enjeu consiste à investir les champs des sciences cognitives et des neurosciences, en vue d'appréhender les mécanismes émotionnels et de décrypter les processus de décision d'achat. Un premier genre d'activité cherche à évaluer au sein de laboratoires l'efficacité d'un message publicitaire, expertisé via la vision de cerveaux en 3D et analysé grâce aux techniques de la neuro-imagerie : « La société française "Impact Mémoire" travaille pour de nombreuses marques sur l'impact du message publicitaire dans la mémoire du consommateur. Cette connaissance intime de la trace laissée par une publicité est très prisée des annonceurs²². » Un deuxième genre d'activité aspire à déchiffrer les fonctionnements cérébraux et à *prédire* les réactions : « Brian Knutson, neuroscientifique de l'université américaine Stanford, a cherché à démontrer qu'il est possible de prédire l'acte d'achat d'une personne en observant l'activation des circuits neuronaux. "Cette expérience marque un tournant. On passe du stade de l'observation à celui de la prédiction. Le neuromarketing entre dans une nouvelle phase", affirme Olivier Oullier, chercheur au CNRS à Marseille et à la Florida Atlantic University²³. »

IBM a développé des logiciels connectés à des caméras vidéo, conçus grâce à ce type de recherches, qui permettent d'analyser en temps réel les désirs et flottements de clients situés dans les espaces de vente : « Il sera possible, en interprétant par exemple les mouvements d'hésitation d'une personne dans un rayon, de déduire qu'elle a besoin d'informations supplémentaires, indique Nicolas Sekkaki, directeur général d'IBM Global Technology Services. Et de commander sur un écran *ad hoc* l'affichage automatique d'un comparateur de prix, d'une fiche technique ou d'un message publicitaire²⁴. » La portée des enjeux financiers induite par les décisions marketing oblige la discipline à maintenir un niveau de performance extrêmement sophistiqué, qui la situe, nous l'avons dit, à l'« avant-garde » de la traçabilité des comportements, raison pour laquelle les agences de renseignement, moins motivées par la quête du profit, s'inspirent souvent dans un second temps de techniques initialement mises au point dans le secteur privé et marchand. « Chaque pensée, et donc chaque intention, est associée à un schéma unique d'activité du cerveau, explique John-Dylan Haynes, chercheur au Max Planck Institute pour les sciences de la cognition et du cerveau. Ainsi, le projet d'une attaque terroriste doit correspondre à un schéma particulier. Si on est capable de le reconnaître, on doit pouvoir prédire que quelqu'un fomenté un tel complot²⁵. » Théories incertaines reprises par

Larry Farwell (qui inspirent certains chercheurs du FBI et de la CIA), selon lesquelles on pourrait désormais reconnaître l'*intention* d'une personne en lisant les images issues d'un *scanning* de son activité cérébrale (*brain fingerprinting*). Conceptions neuromarketing et *dispositifs sécuritaires anticipatoires* s'associent dans la même ambition démiurgique de pénétrer le psychisme des individus – orientation majeure de la surveillance contemporaine, prioritairement programmée par la puissance de l'économie libérale aussitôt capitalisée par le renseignement antiterroriste²⁶.

« Réseaux sociaux »

La popularisation récente et globale des « réseaux sociaux » engendre la production volontaire de masses de données extrêmement individualisées, spécifiées par chaque membre appelé à définir son profil, et dont la plus grande précision permettra une mise en relation pertinente avec de nouveaux « amis ». Informations dont la valeur commerciale pousse notamment les deux sites communautaires les plus importants, Facebook et MySpace, à offrir aux annonceurs l'accès à ces « portraits haute définition ». Facebook Ads, par exemple, constitue un système de signalement publicitaire transmis aux adhérents, en fonction de leurs actions et échanges sur le site, de leurs goûts et pratiques, parfois de leurs orientations sexuelles ou de leurs affiliations politiques et religieuses. « Nous allons aider vos marques à faire partie des conversations quotidiennes qui se produisent tous les jours entre les membres », avait déclaré Mark Zuckerberg, le P-DG, à l'occasion d'une conférence de presse révélant ce projet fondé sur une hypersingularisation systématisée et évolutive des usagers.

Le protocole permet aux régies publicitaires de cibler précisément la diffusion de leurs campagnes dans les pages du réseau en sélectionnant un ensemble de critères : lieu de résidence, genre, âge, situation familiale... Mark Zuckerberg affirme que « le temps de la publicité massive appartient à une histoire révolue » ; désormais, la transmission de messages « d'ami à ami » représente le futur de la communication : « rien n'influence plus quelqu'un que la recommandation d'un ami ». MySpace, ou Google via son outil de messagerie Gmail, développent des procédés similaires sous la forme d'envois de publicités appropriées. Même si les abonnés sont supposés pouvoir refuser ces ingérences continues, la marchandisation des données hypersingularisées constitue un des grands enjeux économiques et juridiques présents et à venir, qui non seulement rétrécit le champ de la vie privée dont une part *s'expose publiquement*, mais réduit encore chacun à une *modulation informationnelle ininterrompue*, dont le traitement fait l'objet d'une *propriété* détenue par un tiers et de transactions opérées avec d'autres tiers. Diagrammes qui revêtent la valeur d'un nouvel « or dématérialisé », indispensable à la rotation à flux tendus et ajustée des biens et des services, à cycle court et à écoulements à la fois *globaux* et *personnalisés*.

La crainte que la saturation d'offres ne lasse les consommateurs encourager certaines sociétés à concevoir des stratégies fondées sur une pleine *complicité* avec les internautes, disposés à diffuser *volontairement* les traces de leurs déplacements sur le Web. Une start-up californienne, Agloco, a développé un protocole à double fonctionnalité : une barre d'outil intégrée au navigateur Internet enregistre la totalité des connexions et transmet simultanément les annonces publicitaires en fonction des profils qui ne cessent de s'affiner. La société reverse quatre-vingt-dix pour cent des recettes aux utilisateurs. Comble de la science marketing qui associe les individus sous forme d'*intéressement*, les absorbe au sein d'un processus « intégral » capable à la fois de motiver les usagers, de récolter des informations présumées fiables et « sans rupture », et de permettre aux annonceurs la transmission d'annonces dénuées de « perte » ou de « bruit ». Le rêve de briser l'écart entre clients et marques se réalise par un *partage mutualisé* des gains, opéré grâce à une radiographie délibérée des pratiques. À l'intérieur d'un ensemble commun où puissance libidinale d'écoulement et appétit de consommation se répondent en un écho immédiat et harmonieux, par le fait d'un traitement consenti et délégué des données personnelles et des alertes publicitaires à un robot tiers, capable de *rapprocher* le plus pertinemment possible demandes singulières et offres adaptées, dans un nouvel environnement marchand toujours plus *ajusté* ou prétendu « vierge de toute disjonction ».

Marketing et sécurité nationale

Non seulement les agences nationales de sécurité s'inspirent presque « en temps réel » des méthodes de traçabilité mises au point dans les laboratoires marketing, mais elles acquièrent également des fichiers auprès de « *data agregators* » – principalement aux États-Unis, où les lois interdisent aux organismes publics la récolte directe, mais non l'achat de données personnelles à caractère commercial. Les sociétés américaines Acxiom, ChoicePoint, LexisNexis opèrent sans restrictions légales la collecte d'informations provenant de sources éparses : connexions Internet, transactions bancaires, déplacements, assurances médicales... Ces « partenariats » confirment les proximités entre stratégies publicitaires et sécuritaires, suivant une sorte de « délégation » implicite accordée au secteur privé, qui *autorise* une cartographie bien plus précise des comportements. Apparition d'une nouvelle forme de *surveillance distribuée* où chaque champ est géré par les compétences les plus adéquates, qui vise un suivi ininterrompu des actions quotidiennes suivant un télescope tendancielllement intégral. « Les dirigeants d'Acxiom sont prêts à aider le gouvernement américain à repérer les fichiers commerciaux les plus utiles et à constituer une base de données géante couvrant les transactions commerciales dans le monde²⁷. »

Cet élargissement du spectre d'observation permis par l'entrecroisement

entre données sécuritaires et commerciales doit à la fois être perçu comme une nette aggravation du traçage des actes quotidiens – sans commune mesure avec la période somme toute récente, où renseignement et marketing constituaient deux activités parallèles qui en quelque sorte s’ignoraient – et comme un moment historique *provisoire*, avant la réalisation possible d’une ambition bien plus démesurée et à la nomination déjà fixée : *agrégation globale de données*. Gigantesque dispositif qui viserait l’extraction et l’analyse d’informations provenant de sources les plus *hétérogènes*. Rêve d’une cartographie des individus, supposée globale et dressée à flux tendus, dont la dissémination de la totalité des traces serait sans fin moissonnée par des systèmes experts *centralisés*. Architecture jusqu’à maintenant illégale dans l’ensemble des pays, et techniquement encore difficile à mettre en place. Néanmoins la pression induite par les incertitudes géopolitiques et les menaces terroristes diffuses, associée à l’augmentation exponentielle des puissances de calcul, peut à terme supposer probable l’achèvement d’une telle « arme de pénétration massive » des êtres, de leurs actions, de leurs intentions : les informaticiens de la NSA travaillent à la mise au point d’ordinateurs capables d’effectuer 10^{24} opérations par seconde, c’est-à-dire un million de milliards de milliards d’opérations par seconde ! Ce qui fait dire à John L. Petersen, président de l’Arlington Institute, un groupe de réflexion spécialisé dans l’impact des nouvelles technologies : « Nous pourrions anticiper le futur grâce à l’interconnexion de toutes les informations vous concernant. Demain, nous saurons tout de vous²⁸. »

Une telle entreprise intitulée « LifeLog Project » avait déjà été initiée par la DARPA²⁹, agence de recherche du département américain de la Défense, qui avait élaboré un prototype de collecte du plus grand volume d’informations produites par chaque individu : connexions Internet, achats et déplacements, retraits bancaires, repérages GPS, appels téléphoniques, programmes de télévision visionnés, capteurs sonores incorporés destinés à enregistrer paroles émises ou entendues, biopuces implantées aptes à signaler certains états de santé... Données captées de toutes parts, réduisant toute personne autant que son réseau relationnel à une maille complexe perpétuellement *quantifiée*. De nombreuses protestations s’élevèrent contre ce projet expérimental, qui conduisirent finalement à son annulation. Preuve que des effets de conscience et de vigilance déployés de la part d’organismes indépendants ou de citoyens peuvent encore contrarier des desseins jugés abusivement intrusifs et politiquement illégitimes. Dimension qui doit particulièrement être soulignée en cette fin de première décennie du XXI^e siècle, dans la mesure où la puissance de ces mécanismes n’est pas encore légalement entièrement validée. Un espace de *délibération* et de renforcement des cadres juridiques demeure ouvert et appelle l’élaboration de postures collectives et individuelles appropriées, à la mesure des bouleversements que l’usage généralisé de l’*agrégation globale de données*

provoquerait dans la vie sociale et dans la vie intime des personnes.

Néanmoins, les serveurs restent dispersés et une « méta-liaison » ne correspond *pas encore* à la réalité de l'accès aux données. Une extrême *fragmentation* caractérise les stockages informationnels, qui rend pour l'instant cette ambition panoptique impossible, mais un double mouvement – économique et politique – tend à créer les conditions possibles de son avènement qui, s'il s'accomplissait, exposerait un tout autre paradigme dans la cartographie des individus. Un seuil définitif serait franchi qui repousserait « trous » et « vides » qui jusqu'à maintenant *brouillent* la capacité d'un suivi en continu, au profit d'une *radiographie intégrale*, par une récolte ininterrompue et « sans rupture » des renseignements générés par les comportements. Portraits haute définition et quasiment *complets*, permettant quantité de *déductions*, réduisant la vie de chacun à une *somme informationnelle* à disposition d'organismes commerciaux et de sécurité. « Il pensa au télécran et à son oreille toujours ouverte. Ils pouvaient vous espionner nuit et jour, mais si l'on ne perdait pas la tête, on pouvait les déjouer³⁰. » Cette réflexion de Winston Smith, héros encerclé de toutes parts dans le roman de George Orwell, pourrait être reformulée presque à l'identique par chacun de nous (à la nuance près qu'il faudrait substituer aux « télécrans » les « bases de données »). Mais resterait à l'esprit la menace croissante – en l'absence d'une vigilance active de notre part – de ne pouvoir bientôt « déjouer » l'intrusivité globale produite par l'agrégation fatale et définitive de l'ensemble de nos traces.

Ce qui est désormais nommé « dataveillance », c'est-à-dire l'achèvement de la forme majeure de surveillance, fondée sur l'interception et le traitement de données, constitue, nous l'avons vu, le pivot central de la modalité d'observation des activités quotidiennes. Elle ne représente pas une branche parmi d'autres, mais profite de la réduction à des codes numériques de la quasi-totalité des informations récoltées de toutes parts (vidéosurveillance, géolocalisation, biométrie, capteurs, navigations Internet...), en vue de traiter ces sources hétérogènes dans l'intention de dresser des profils toujours plus précis et continus grâce à la *complémentarité* des renseignements. L'analyse des données occupe le point d'articulation décisif d'observation : d'un côté située au bout de la chaîne des traces recueillies, et d'un autre côté située en amont des procédures d'alerte. Position nodale qui lui octroie une puissance de pénétration sans cesse perfectionnée, probablement appelée un jour à « envelopper » tout individu sans coupure spatiale et temporelle.

Il n'est pas certain que nos sociétés aient perçu la pleine mesure des nouvelles instances de *pouvoir* que représentent les centrales de gestion des données personnelles. Il est probable que se joue – selon les contraintes réglementaires qui leur seront opposées ou non – l'avenir de la vitalité démocratique, de la pérennité des libertés publiques et du droit à la vie privée. C'est exactement à l'intérieur de ce moment historique, où les configurations

ne sont pas encore définitivement fixées, que doivent se concevoir des stratégies destinées à encadrer pertinemment l'usage des traces disséminées par chacun. Enjeux politiques et sociaux majeurs, qui étrangement ne suscitent aucun effet de conscience proportionnel aux menaces potentielles. Comme l'avait observé le juge Brennan, « la liberté est fragile. [...] De même que la nuit ne tombe pas brusquement, il en est de même de l'oppression. Dans les deux cas, il y a d'abord un crépuscule pendant lequel rien ne semble changer. Or, c'est pendant le crépuscule qu'il faut se soucier des changements qui se produisent³¹ ». L'*ambivalence fonctionnelle* des objets numériques (à la fois applications positives et machines de traçabilité) constitue peut-être la cause d'une indifférence généralisée et inquiétante ; l'*invisibilité* des traces renforce encore ces phénomènes d'apathie.

Seuls des efforts de description et d'analyse auxquels cet ouvrage s'efforce de contribuer, ou des mises en garde émanant d'institutions de veille, peuvent probablement favoriser une nécessaire lucidité collective, susceptible de répliquer par la loi à l'infiltration expansive dans l'intimité psychique des êtres. En France, malgré la dimension prioritairement consultative et non contraignante de la CNIL, son président Alex Türk s'est évertué à plusieurs reprises à alerter l'opinion quant à l'approximation juridique relative à l'usage des données personnelles : « Le capital de notre identité et de notre vie privée est chaque jour menacé. Il y a urgence à le préserver. Comme le capital environnemental de l'humanité, il risque, lui aussi, d'être si gravement atteint qu'il ne puisse être renouvelé. J'appelle au développement d'une convention universelle de protection des données, instrument juridique qui devrait être une grande déclaration de droits, consacrant la reconnaissance d'un droit universel à la protection des données et à la vie privée³². » Un an plus tard, à l'occasion de la présentation du vingt-huitième rapport annuel de la CNIL, Alex Türk affirmait la probable nécessité d'« inscrire en préambule de la Constitution – qui rappelle les droits fondamentaux – la protection des données personnelles³³ ».

L'ensemble de nos traces ne recouvrira jamais exactement nos *singularités*, qui assurément débordent toute réduction algorithmique ; néanmoins, nos « disséminations numériques » composent des atlas suffisamment détaillés pour que la gestion par des sociétés privées ou organismes d'État – enjeu transnational de société majeur de notre temps – fasse l'objet de délibérations publiques à hauteur nationale et globale. L'usage et la finalité des récoltes n'ont pas encore fait l'objet d'encadrements juridiques précis. L'ignorance de la diffusion et de la destination des flux amplifie encore l'écart entre citoyens souvent peu informés et dispositifs techniques extrêmement puissants. La commercialisation de nos « ombres digitales », informations relatives à la vie privée, inscrit l'*identité humaine* comme une marchandise, *ultime objet de transaction* de l'économie libérale, disposée à monnayer ses *planisphères individualisés* à quiconque : instances

financières ou sécuritaires. L'avenir des bases de données consistera à relier en temps réel profil momentané de chacun et réseau d'offres commerciales et médicales adaptées, situées dans une *opportunité* spatio-temporelle *immédiate*, à l'intérieur d'un *halo électronique personnalisé* et permanent où individus et puissances de vente ou d'examen anatomiques seront connectés et interagiront sans fin. *Signalements mutuels* des désirs, des offres et des états de santé, consultables *parallèlement* par les agences de renseignement, capables de suivre à la trace déambulations spatiales, conduites d'achat et conditions thérapeutiques. Architecture appelée à être perfectionnée par l'inscription du *corps* au centre du système, surface désormais *directement* lisible, *interface* privilégiée, au contact de *capteurs biométriques* toujours plus omniprésents et programmés à *identifier, authentifier, tracer*. À l'intérieur d'une matrice intégrale où chaque mouvement sera non seulement repéré et *validé*, mais contribuera aussi à amplifier les flots de données personnelles, classées suivant des *distributions* plus finement différenciées et *spécifiées*, et dont l'*interopérabilité* aux autres types d'information intensifiera la puissance et l'exactitude de la machine universelle de *quantification* spatio-temporelle des individus, désormais envisagés comme des points « organico-électroniques » de traitement et d'évaluation.

1- Cf. André Leroi-Gourhan, *La Mémoire et les Rythmes*, Paris, Albin Michel, 1965 ; voir plus précisément le chapitre IX, « La mémoire en expansion », p. 63-76.

2- Georges Banu, *La Scène surveillée*, Actes Sud, 2006, p. 80.

3- Paris, Le Seuil, 1972.

4- « Un bon souverain, que ce soit un souverain collectif ou individuel, c'est quelqu'un qui est bien placé à l'intérieur d'un territoire, et un territoire qui est bien placé au niveau de son obéissance au souverain est un territoire qui a une bonne disposition spatiale. » (Michel Foucault évoquant les cadres sécuritaires qui régissent les villes à l'âge classique, in *Sécurité, territoire, population*, cours au Collège de France, 1977-1978, Paris, Gallimard/Le Seuil, 2004, p. 16).

5- Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », *L'Autre Journal*, n°1, mai 1990.

6- Michel Foucault, *Surveiller et punir*, op. cit., p. 235.

7- *Le Testament du docteur Mabuse*, réalisé en 1933.

8- Michel Foucault, *Surveiller et punir*, op. cit., p. 236.

9- New York, Paddington Press, 1978.

10- « Lara Srivastava achève son exposé par un dessin humoristique en deux parties. L'une représente un homme d'affaires disant à un individu : "Je veux greffer sur vous un tag RFID. – Cela viole mes droits", répond le consommateur. L'autre reprend la même scène en modifiant le discours : "Je veux greffer sur vous un tag RFID qui est aussi un téléphone mobile, une caméra vidéo et un lecteur MP3. – Cool", répond alors l'individu » (Michel Alberganti, *Sous l'œil des puces. La RFID et la démocratie*, Arles, Actes Sud, 2007, p. 127).

11- Téléchargeable sur : <http://www.ladocumentationfrancaise.fr/rapports-publics/064000885/index.shtml>.

12- Concept développé par François Ascher, déjà évoqué dans le chapitre précédent.

13- « Paradoxal, insaisissable, imprévisible sont les mots le plus souvent employés par les marketeurs depuis les années 2000 pour désigner le comportement du consommateur. Il y a encore dix ans, il suffisait de se baser sur la catégorie socioprofessionnelle pour dérouler le fil de la pelote des habitudes de consommation et même les envies. Las ! L'évolution de nos sociétés modernes montre chaque jour l'obsolescence d'une telle démarche » (Christian Salmon, *Storytelling, la machine à fabriquer des histoires et à formater les esprits*, Paris, La Découverte, 2007, p. 24).

- 14- « À partir du moment où les biens deviennent de simples supports de services et où les services sont le moteur du commerce mondial, la construction de relations avec les consommateurs joue un rôle clé. Dans la nouvelle économie en réseau, le marketing est roi, et le contrôle du consommateur devient l'objectif numéro un de l'activité économique » (Jeremy Rifkin, *L'Âge de l'accès. La nouvelle culture du capitalisme*, Paris, La Découverte, 2000, p. 135).
- 15- Gilles Deleuze, « Post-scriptum sur les sociétés de contrôle », *L'Autre Journal*, n° 1, mai 1990.
- 16- « *My life, my card* : le slogan de la campagne American Express consiste ainsi à associer l'usage de la carte de crédit aux épisodes mémorables de notre vie, jusqu'à faire de l'utilisation de la carte l'un de ces épisodes mêmes » (Christian Salmon, *Storytelling, la machine à fabriquer des histoires et à formater les esprits*, op. cit., p. 42).
- 17- Cité par Annie Kahn, « Avec JCDecaux, l'Inria imagine la publicité sur mesure pour le chaland », *Le Monde*, 31 mars 2006.
- 18- Cité par Laurence Girard, « Le métro parisien s'apprête à accueillir l'affichage interactif », *Le Monde*, 4 octobre 2007.
- 19- Jacques Henno, *Tous fichés, l'incroyable projet américain pour déjouer les attentats terroristes*, op. cit., p. 68.
- 20- *Ibid.*, p. 70.
- 21- *Ibid.*, p. 33-34.
- 22- Laurence Girard, « Les publicitaires s'intéressent à notre cerveau », *Le Monde*, 28 mars 2007.
- 23- *Ibid.*
- 24- Michel Alberganti et Hervé Morin, « Pourra-t-on lire dans nos pensées ? », *Le Monde*, 6 mai 2007.
- 25- *Ibid.*
- 26- La Charte des droits de l'homme du Conseil de l'Europe interdit d'utiliser à des fins de sécurité des données recueillies à titre commercial (principe rarement respecté en Europe et en tout point ignoré aux États-Unis).
- 27- Jacques Henno, *Tous fichés, l'incroyable projet américain pour déjouer les attentats terroristes*, op. cit., p. 124.
- 28- *Ibid.*, p. 77.
- 29- Defence Advanced Research Projects Agency.
- 30- George Orwell, *1984*, op. cit., p. 222.
- 31- Cité par Sophie Body-Gendrot, *La peur détruira-t-elle la ville ?*, Paris, Bourin Éditeur, 2008, p. 56.
- 32- Jean-Marc Manach, « Des moyens insuffisants et des défis nombreux : la difficile équation de la CNIL », *Le Monde*, 21 avril 2007.
- 33- « La CNIL veut inscrire dans la Constitution la protection des données personnelles », *Le Monde*, 16 mai 2008.

V BIOMÉTRIE

Le corps indexé

Double régime provisoire

Au début du film de Ridley Scott *Blade Runner* (1982), un inspecteur procède à la décomposition automatique d'un iris en vue de repérer les *replicants*, androïdes devenus menaçants, que rien ne permet de distinguer des humains. Dans une scène ultérieure, Rick Deckard, le *blade runner* chargé d'éliminer les robots humanoïdes – joué par Harrison Ford –, pénètre dans un espace via un processus de reconnaissance vocale. Plus tard, on le voit insérer une carte dans un lecteur lui permettant d'intégrer le hall d'un immeuble. Régime hybride où les identifications s'opèrent à la fois par l'analyse de certaines parties du corps et par le port d'un badge adéquat. Le scénario adapté d'une nouvelle de Philip K. Dick¹ situe l'action en 2019, période très éloignée de la date de rédaction qui autorise toutes les hypothèses de science-fiction. Ce moment-là pourrait exactement caractériser notre temps historique, à l'intérieur duquel usage de documents électroniques et scannage de la peau conditionnent les procédures actuelles d'authentification des individus. Néanmoins, on peut supposer sans risque que d'ici 2019 cette double dimension se sera « simplifiée » au profit d'une *exclusive* vérification des identités exécutée par des systèmes biométriques.

La biométrie peut être définie comme la « science du calcul des dimensions d'un organe humain », qui cherche à transformer certaines caractéristiques physiques du corps (doigts, main, visage, iris, rétine...) en une « empreinte numérique » ou série de codes binaires. L'objectif vise l'authentification et/ou l'identification des personnes. Les données collectées doivent être *universelles* (exister chez tous les êtres), *uniques* (permettre de différencier les individus), *permanentes* (autoriser l'évolution dans le temps), *enregistrables* (capter les informations, généralement avec l'assentiment) et *mesurables* (rendre viable une comparaison future). La technique consiste en deux types de contrôles : évaluation physique ou comportementale, et reconnaît jusqu'à maintenant six procédés : empreintes digitales et palmaires,

analyse de l'iris et de la rétine, reconnaissance faciale, configuration des veines (la reconnaissance vocale s'inscrit d'une certaine façon à l'intérieur d'un autre champ de recherche).

Procédés multiples

Différents protocoles auscultent des fragments spécifiques de l'organisme. La lecture biométrique des *empreintes digitales* demeure la technique généralement privilégiée. Alphonse Bertillon, directeur du service de l'identité judiciaire au début du XX^e siècle, avait établi la singularité absolue des lignes des doigts pour chaque individu. Permanentes et uniques, elles sont formées avant la naissance et leur dessin subsiste à l'identique durant l'existence. La comparaison d'une empreinte électronique s'effectue en moins d'une seconde ; le taux de rejet (erreur d'identification) est extrêmement faible. La *géométrie de la main (hand-scan)* consiste à mesurer plusieurs caractéristiques (presque une centaine) telles que forme, longueur et largeur des doigts, contours des articulations... Le système présente des FAR (*False Acceptation Rates*) assez élevés, particulièrement entre personnes d'une même famille ou entre jumeaux, par exemple. *L'identification par l'iris* effectue la saisie initiale d'un très grand nombre de points qui ne varient quasiment pas durant la vie d'une personne. Ce procédé recouvre l'inconvénient de nécessiter un éclairage adéquat et peut encourager des fraudes, notamment par l'usage de lentilles. Néanmoins, ce principe offre une fiabilité, dans la mesure où plus de deux cent quarante points sont retenus contre environ quatre-vingts pour l'empreinte digitale. *L'identification de la rétine (retina-scan)* se base sur le schéma formé par les vaisseaux sanguins de la paroi interne de l'œil – unique pour chaque individu et assez stable au cours de la vie. Elle semble moins bien acceptée par les utilisateurs par le fait de son caractère trop contraignant : la mesure doit s'effectuer à faible distance du capteur (quelques centimètres) pour que le balayage soit réussi. La mesure rétinienne est la plus difficile à réaliser mais également la plus compliquée à contrefaire.

La *reconnaissance du visage (facial-scan)* consiste à analyser un ensemble de facteurs supposés invariables : haut des joues, coins de la bouche, et à éviter les surfaces occupées par les cheveux ou les zones sujettes à modification au cours des âges. Malgré un taux d'erreurs important, la technique s'améliore et se précise peu à peu. La *configuration des veines (vein pattern-scan)*, habituellement combinée à la géométrie de la main, décompose le dessin formé par le réseau des veines en se focalisant sur quelques points caractéristiques. Par exemple, le groupe japonais Fujitsu a conçu un boîtier, nommé *PalmSecure*, qui identifie une personne par les veines de sa paume. Quelques banques ont adopté cette technologie pour les retraits de billets : l'utilisateur pose sa main sur l'appareil ; illuminée par une lumière infrarouge, l'hémoglobine des vaisseaux palmaires absorbe ces rayons, réduisant leur

réflexion. En quelques secondes, la photographie numérique obtenue peut être comparée aux données archivées dans les fichiers. Enfin, la *reconnaissance vocale* (*voice-scan*), qui n'analyse pas une partie du corps mais une de ses manifestations, examine tonalité et fréquence de la voix ainsi que la distance entre la formation des phonèmes. Elle peut distinguer un homme d'une femme, mais reste dépendante de la qualité de l'enregistrement et du type de message.

Les données recueillies proviennent de caractéristiques à la fois physiologiques et comportementales qui ne sont en général pas imitables. Plusieurs autres formules sont en cours de développement : géométrie de l'oreille, dessin des lèvres, forme des pores de la peau, analyses de traces biologiques (odeurs, ADN, salive, sang...), suivant un spectre de potentialités correspondant à toutes les dimensions constantes et mesurables du corps. La multiplicité des procédés témoigne probablement, en creux, de leur *faillibilité* (plus ou moins marquée selon les méthodes employées). Chaque technique paraît offrir avantages et inconvénients, d'abord par le fait de la modification inéluctable de certaines parties de l'organisme, ensuite par le fait de falsifications possibles. Aucune des évaluations opérées ne se révèle totalement parfaite : le corps s'adapte à l'environnement, vieillit, subit des traumatismes troublant la pérennité des données archivées. Néanmoins, les systèmes sont conçus pour autoriser une marge d'erreurs acceptable entre la mesure et la référence, afin d'éviter que tout écart mineur n'invalide l'identification et rende les capteurs biométriques inutilisables à grande échelle. En outre, il est concevable de fabriquer une « fausse empreinte » à partir d'une trace recueillie sur un verre, un clavier, une poignée..., au moyen d'une couche de silicone reproduisant la géométrie du doigt. Enfin, les données biométriques sont constituées de codes numériques susceptibles d'être infiltrés sur des serveurs, et ensuite dupliqués en vue de créer des « prothèses dédoublées », admissibles aux yeux des capteurs.

Le film *Bienvenue à Gattaca* d'Andrew Niccol (1998) montre comment les salariés d'une entreprise « sensible », spécialisée dans le lancement de satellites spatiaux, sont constamment soumis à des contrôles biométriques ou tests ADN pour accéder aux espaces de travail et maintenir un « haut degré de compétence ». Un jeune homme ne correspondant pas aux canons génétiques scelle un accord avec une personne conforme aux critères, mais frappée d'une invalidité tétraplégique et donc incapable d'assumer une activité professionnelle physiquement exigeante. Le premier reçoit quotidiennement du second des fragments de son corps (urine, sang, cheveux) afin qu'il puisse lui substituer son identité et intégrer la compagnie. Stratégie qui parvient à déjouer un système à l'apparence parfaite. Il est probable que la biométrie contemporaine bénéficie d'une même aura supposée infaillible, alors que son efficacité – notamment dans les mesures de masses – ne se vérifie pas exactement dans les faits.

Il est encore plausible d'avancer que les budgets sans cesse croissants aient été dépensés en pure perte, non seulement parce que certains dispositifs attestent régulièrement de déficiences, mais encore parce que la biométrie n'aura probablement formé qu'une brève parenthèse dans l'histoire de la surveillance, vite supplantée par la généralisation universelle d'*implants* dans les corps, à la fois plus fiables et offrant des fonctionnalités plus nombreuses et plus puissantes (suivi des déplacements, communications, achats, états de santé, régimes alimentaires...). À ce jour, les sociétés civiles ne semblent pas encore disposées à accepter une telle intrusivité à l'intérieur de l'organisme (pénétration d'une certaine façon déjà à l'œuvre, nous l'avons vu, mais sans réelle manifestation sensible – tout au contraire même – et qui se déploie par effets d'invisibilité et dans l'ignorance de la dissémination et de la destination des traces). Néanmoins, les technologies biométriques continuent de se développer et de se perfectionner, imposant des relations entre êtres et machines fondées sur la *vérification* continue des identités et la *mémorisation* d'un nombre toujours plus étendu de déplacements et d'actions quotidiennes.

Extension universelle

Un système biométrique fonctionne selon deux architectures. La première permet l'authentification d'un individu grâce au croisement de l'analyse d'une partie du corps et d'informations correspondantes stockées sur une carte à puce, portée par son détenteur ; l'adéquation est vérifiée entre les deux « sources ». La seconde approche consiste à centraliser les données biométriques ; le système va rechercher dans une base de données les références de la personne contrôlée. L'une correspond à une *biométrie sans trace*, l'autre à une *biométrie à trace*. Quelle que soit la modalité, les objectifs visés sont multiples : éviter le doute relativement aux identités ; autoriser un accès ou une opération exclusivement à une personne dont les données physiques auront été préalablement saisies et enregistrées, et, enfin, supprimer l'usage des mots de passe. S'est opérée depuis quelques années une extension progressive des identificateurs biométriques suivant une densité spatiale toujours plus resserrée : aéroports, entreprises, administrations... Parallèlement à ces infiltrations à utilisations collectives, s'est développé un usage privatif de mini-lecteurs d'empreintes digitales qui se sont progressivement intégrés dans divers objets du quotidien : attachés-cases, clés USB, disques durs externes, souris d'ordinateur... Certains véhicules couplent, par exemple, ouverture des portières et mise du contact par scannage biométrique. Les applications dans le commerce électronique font l'objet de recherches et de tests de fiabilité ; à terme, elles seraient supposées sécuriser davantage les transactions en ligne, mais amplifieront surtout le volume d'*informations biométriques disséminées* dans les réseaux.

En 2006, durant la Coupe du monde de football en Allemagne, les forces de police avaient mis en place un système à grande échelle, permettant

l'identification de personnes ayant commis par le passé des actes de violence dans le cadre de manifestations sportives : les empreintes digitales étaient saisies par un scanner à l'entrée des stades, comparées en temps réel avec les bases de données du Land concerné ou avec celles des services fédéraux de la police judiciaire. Machine de filtrage de masse, fondée sur la mémorisation des antécédents et physiquement incontournable. D'autres dispositifs destinés à des utilisations massives requièrent pour leur part l'assentiment des usagers, à l'instar du programme Inspass (*Immigration and Naturalization Service Passenger Accelerated Service System*), qui permet aux « voyageurs fréquents » de ne pas avoir à présenter leurs documents d'identité à la douane de certains aéroports internationaux (Los Angeles, Miami, New York, Washington, Toronto, Vancouver...). Des milliers de personnes se portent volontaires dans le but de gagner du temps, qui sont probablement indifférentes à la précise cartographie spatio-temporelle qui se constitue relativement à leurs trajets. Certains établissements scolaires installent des dispositifs biométriques afin d'éviter l'introduction dans leurs locaux d'éléments étrangers susceptibles de commettre des exactions.

La *biométrie comportementale*, fondée sur l'analyse caractéristique des gestes et leur reconnaissance, constitue une autre branche de recherche et d'application. Par exemple, la *dynamique de signature* (*signature-scan*) mesure au moyen d'un stylo équipé d'un capteur la nature du mouvement (vitesse, pression et accélérations, durée d'exécution...). Technique encore peu utilisée mais qui pourrait s'étendre à des usages spécifiques (documents électroniques, rapports, contrats...). La *dynamique de frappes de clavier* consiste à valider ou non l'authentification d'une personne avant la réalisation d'opérations sur ordinateur ou en ligne, ou encore à « expertiser la gestion du temps de travail », par évaluation des durées entre les tapes ou la fréquence des erreurs. L'hétérogénéité des techniques déjà à l'œuvre et de celles à venir confirme la densification protéiforme de la *maille sensible* qui analysera nos gestes, appelés à être examinés sans relâche par la « lecture » automatisée de nos fragments anatomiques et par l'estimation robotisée de nos attitudes à des fins d'identification, de repérage spatial ou de « mesure de qualité ».

Future « biotransparence »

Le concept d'*altérité* « identifié » par Emmanuel Lévinas dans l'absolue singularité de chaque « visage » subit ici un déplacement, n'étant plus envisagé comme l'évidence de la différence qui appelle par son écart même la possibilité de la relation, mais comme une « présence muette » devant préalablement être *vérifiée* avant d'autoriser une action ou un accès. Le rapport à l'autre ne s'instaure plus dans la béance et la surprise de la rencontre mais se *règle* d'après un processus de *conformation robotisée*. Le corps s'expose comme une *surface informationnelle* scannée et *indexée* – non plus sujette à la vision (régime de la vidéosurveillance) mais au *toucher*

(découpage systématisé) de l'anatomie – à l'intérieur d'un espace global toujours plus continu et « lisse », « haptique », selon les termes de Deleuze qui le distingue de l'espace « strié » qui, lui, relèverait d'une incontournable mise à distance *optique*, imposée par l'opposition frontale entre les visages. *Enveloppement* des corps par des « palpeurs » électroniques, attestant de la *concordance* de chacun en regard de finalités sociales déjà programmées et bientôt *universellement* inévitables.

Un autre concept, celui de *biopolitique*, élaboré par Foucault, distingue l'apparition, vers le milieu du XVIII^e siècle, d'une forme d'exercice du pouvoir qui porte non plus sur les territoires et leur quadrillage administratif et sécuritaire mais sur la qualité biologique des populations, laquelle requiert un relevé régulier des états sanitaires individuels et collectifs, faisant ainsi l'objet d'une « anatomie politique » soucieuse d'un bon ordonnancement hygiénique, supposé nécessaire au maintien de l'ordre moral et à l'efficacité économique de la société. Taux de natalité et de mortalité, pyramide des âges, recension et prévention des maladies, autant d'attentions et d'informations qui visent à se prémunir de tout désordre potentiellement immaîtrisable et à optimiser la force collective. Le développement des nanotechnologies et l'intégration, dans les tissus humains, de processeurs capables de mesurer les flux biotiques et de transmettre en temps réel les données à des organismes médicaux ou autres (employeurs, écoles, assurances...) achèveront cette ambition de *totale transparence* des corps, en exposant à *vie* une dissection *partagée* de l'activité organique (alimentation, allergies, états émotionnels...) inscrivant l'*intimité biologique* comme une information *accessible* à quantité de *tiers*. La *biométrie* préfigurerait, davantage qu'une technique, un *concept intermédiaire* entre une *biopolitique* inquiète d'une nécessaire hygiène médicale, et une *biotransparence* – future connaissance multicritères et à *flux tendus* des processus physiologiques individuels –, suivant un ordre qui cherche d'abord à *quantifier* non les fréquences vitales mais la *concordance* entre corps et état civil.

L'abandon progressif de la *dimension déclarative* constitue une rupture qui brise le pacte de confiance qui liait État et citoyens, au profit de la même logique de *suspicion* que nous avons déjà signalée à plusieurs reprises. Une identification/authentification automatisée et en théorie « infalsifiable », non seulement se substitue à l'*énonciation libre* de son identité, mais autorise encore la mise en réseau des informations à d'autres masses de données hétérogènes, contribuant ainsi à compléter un tableau déjà hautement détaillé des comportements. Un autre mode de relations interpersonnelles et d'intrusivité s'instaure : indifférence généralisée à l'égard de la parole émise / indexation numérisée et archivée des substances organiques / mémorisation des circulations physiques et de nombreux types d'opérations. La *biométrie* situe chaque être humain comme une « surface muette » sans fin appelée à se soumettre à des procédures de *vérification*, dans

une négation de la notion de *pacte*, en partie fondatrice du principe de socialisation moderne. Dimensions qui se seront davantage universalisées, systématisées, et devenues en tous points incontournables à l'âge *postérieur* marqué par les nanopuces et une *biotransparence* globale.

Peut-être une parade possible consisterait-elle à adopter la stratégie des services de renseignement qu'on voit œuvrer dans le film de Richard Linklater *A Scanner Darkly* (2006), une fois encore adapté d'une nouvelle éponyme de Philip K. Dick², consistant à porter les combinaisons conçues par des « designers génétiques », qui modifient en permanence l'apparence humaine, interdisant *de facto* de stabiliser une forme reconnaissable³. Utopie irréalisable qui témoigne de la difficulté présente et à venir de se soustraire à ce nouveau régime provisoire mais implacable de mesure d'authenticité et d'acceptabilité des êtres. L'extension du nombre de documents d'identité biométriques marque dans les faits la généralisation du principe d'identification automatisée des personnes par une infinité de capteurs, inscrivant le corps comme un point physique d'émission de flux électroniques destinés à être analysés, stockés et croisés dans la mesure du possible à toutes ses *autres traces relatives*.

De nombreux pays adoptent et imposent progressivement le port de cartes d'identité et de passeports biométriques (soit à l'égard de leurs ressortissants, soit à l'égard de voyageurs étrangers appelés à entrer sur leur territoire). En France, le projet INES (Identité nationale électronique sécurisée), en partie modifié à la suite de débats publics et de forums de discussions sur Internet, prévoit que la carte comprendra une puce lisible sans contact (limitée à une distance d'environ un centimètre) dans laquelle seront stockés état civil, photo numérisée, et six à huit des empreintes digitales du titulaire. Elle ne sera pas obligatoire, contrairement à ce qui avait été envisagé en première instance. Elle suppose la mise en place de quatre bases de données nationales : état civil des ressortissants français, empreintes digitales, images faciales numérisées, références des détenteurs des nouveaux passeports. La centralisation des renseignements répond à une exigence régulièrement formulée par les services de police qui souhaitent pouvoir pratiquer des contrôles capables de « remonter » d'une empreinte digitale anonyme vers la distinction de son « signataire ». Certaines associations avaient plaidé pour que le système soit décentralisé et pour qu'il stocke les données biométriques localement sur la puce, option finalement écartée par les concepteurs du projet qui ont argué la nécessité d'une base centrale, seule capable de vérifier qu'une même personne ne dispose pas d'identités multiples, et, à l'inverse, qu'une seule identité n'a pas été attribuée à plusieurs reprises.

Outre que cette procédure de recoupement participe d'une extension de l'interconnexion entre bases de données administratives et sécuritaires, elle suppose encore un *usage dérivé* de fonctions initialement destinées à attester seulement de l'identité d'une personne. Il s'opère une systématisation de la

« logique des traces » (ADN, empreintes digitales...) qui affaiblit la notion d'« espace public anonyme » au profit de la constitution d'une *zone globale sensible* infiltrée de capteurs connectés à de multiples bases de données. Détournements des applications légitimés par le souci de sécurité publique, qu'on prétend « indolores » pour celles et ceux n'ayant commis aucun délit, mais qui induisent une utilisation accordée *in fine* aux instances étatiques de surveillance, autorisées à *orienter* les motivations d'origine à d'autres fins, conformément à un inconscient collectif hypertrophié depuis le 11 septembre 2001, qui veut que rien ne doit être refusé à l'exigence de « protection » des citoyens. Pratiques souvent consenties sans validation législative, à l'intérieur d'un récent et discret *régime d'exception* expansif qui redistribue « sous la contrainte des événements » l'ordre des priorités politiques et sociales : « Conformément à une tendance en acte dans toutes les démocraties occidentales, la déclaration de l'état d'exception est progressivement remplacée par une généralisation sans précédent du paradigme de la sécurité comme technique normale de gouvernement⁴. »

L'objectif majeur du dispositif consiste à éviter les fraudes à l'identité et à tendre vers la plus grande fiabilité et sécurisation des titres. But *a priori* louable, mais qui entraîne avec sa réalisation quantité d'effets collatéraux qui s'additionnent à d'autres simultanément produits par les protocoles déjà évoqués, pour finalement se multiplier et se « potentialiser » entre eux. Qui perturbent toujours plus violemment le droit historique des individus à maintenir une part de leur existence à l'abri d'instruments automatisés de repérage en temps réel de leurs conduites et de leurs référencements civils – de surcroît toujours susceptibles d'être connectés à d'autres sources, marketing ou professionnelles par exemple. Cependant, malgré les craintes suscitées par les cartes équipées de puces lisibles sans contact (à l'instar du « passe Navigo » commercialisé par la RATP), ces dernières ne pourraient pas, jusqu'à maintenant du moins, techniquement et légalement laisser supposer des contrôles d'identité à l'insu des intéressés par des myriades de capteurs dissimulés.

Dimension appelée à coup sûr à se matérialiser par la généralisation des biopuces, *saut ultérieur* dans la *traçabilité intégrale* des individus, aux conséquences juridiques et éthiques abyssales, dont les sociétés contemporaines devront bien prendre la véritable *mesure*. Architecture implacable contre laquelle il demeure encore possible d'élaborer des stratégies d'information et d'action, capables d'exposer publiquement la complexité des menaces et des enjeux que suppose la pénétration de composants électroniques et géolocalisés dans les corps du XXI^e siècle. La biométrie forme une *autre strate* au sein de l'architecture globale de collecte de données, *distribuée* suivant des procédures multiples. Outre celles explorées jusque-là, d'autres systèmes encore se complètent ou se *relaient* dans la *maille universelle et multicouches* : interception à grande échelle de

communications ou introduction récente et expansive de puces électroniques à l'intérieur d'objets du quotidien, désormais capables d'être suivis *à la trace* et de *témoigner* de leur « physiologie » ou de leurs *usages*.

1- *Les androïdes rêvent-ils de moutons électriques ?*, Paris, Lattès, 1979 (nouvelle renommée *Blade Runner* à la suite du film de Ridley Scott).

2- Philip K. Dick, *Substance Mort*, Paris, Denoël, 1978.

3- « Apparemment personne ne connaît son aspect ; il doit changer de canevas physiognomonique tous les mois » (Philip K. Dick, *Ubik*, Paris, Robert Laffont, « 10-18 », 1970, p. 8).

4- Giorgio Agamben, *État d'exception*, *Homo Sacer*, *op. cit.*, p. 29.

VI

INTERCEPTION DES COMMUNICATIONS

/ PUCES RFID / NANOTECHNOLOGIES

Du télescope au « nanoscope »

Ambitions intégrales

Une multiplicité de modalités de collectes informationnelles infiltrent notre environnement, dont l'efficacité semble inversement proportionnelle à leur échelle. Le mégasystème *Echelon*, premier réseau planétaire d'interception de communications internationales par satellite (conversations téléphoniques, SMS, navigation Internet, courriers électroniques), correspond à un dispositif monumental mis en place dans l'après-guerre. Maille multipolaire composée de stations d'écoute disséminées dans une dizaine de pays, dont l'origine remonte au pacte Ukusa signé en 1948 entre les États-Unis et leurs alliés anglophones (Royaume-Uni, Canada, Australie, Nouvelle-Zélande). La France, l'Allemagne, la Russie utilisent des observatoires similaires mais de moindre envergure, de même que certains États du Moyen-Orient (Israël, Arabie Saoudite, pays du Golfe). *Echelon* pourrait happer trois milliards de communications par jour, via des processus complexes de technologies de filtrage (*filtering technologies*) et capterait environ 90 % du trafic Internet, mais n'en analyserait finalement qu'une minorité. Le 20 décembre 2001, un citoyen britannique, Richard Reid, tenta, sur un vol Paris-Miami, de mettre à feu des explosifs qu'il avait dissimulés dans ses chaussures. La soirée précédente, des emails avaient été échangés, à partir d'un cybercafé parisien, entre Reid et ses donneurs d'ordres situés au Pakistan, sans qu'aucun algorithme n'ait surpris ces correspondances.

Probablement cet événement – parmi d'autres – témoigne-t-il de la *vanité* ou de l'obsolescence de ces machines démesurées, incapables *in fine* de répondre à l'ambition de réaliser une couverture globale. L'analyse individualisée des traces comportementales – que nous avons explorée plus haut – correspond davantage aux modes sophistiqués de prévention supposée des menaces par la constitution universalisée de profils singuliers et multicritères. Ces mécanismes d'écoute à échelle planétaire sont contraires à

la Déclaration universelle des droits de l'homme, à la Convention européenne des droits de l'homme et à la Convention sur les télécommunications internationales, censées garantir la confidentialité des échanges ; restrictions qui concourent à compliquer une extension continue de ces gigantesques et fragiles tentacules. Néanmoins, ces observatoires initialement destinés à répondre à des objectifs strictement militaires ont opéré depuis une sorte de reconversion majoritairement orientée vers l'espionnage économique. De grandes entreprises américaines et anglo-saxonnes bénéficient d'informations susceptibles de moduler les négociations en fonction de la connaissance des positions concurrentes. Confirmation renouvelée de l'étroitesse des liens qui lient pouvoirs militaires et financiers, sous la forme d'une *guerre économique* globale, d'abord fondée sur la qualité des informations récoltées.

La NSA (National Security Agency) – la plus importante des seize agences de renseignement américaines – disposerait d'un budget dix fois supérieur à celui de la CIA, mais non rendu public. Elle concevrait elle-même certains de ses supercalculateurs ou d'autres technologies appelées à demeurer secrètes. Surnommée « Crypto City », elle se situe non loin de Washington ; la bannière géante posée sur son fronton affirme qu'elle « ne reculera jamais ». Ses services collectent des millions de communications mais ne peuvent, dans les faits, analyser ou interpréter la totalité des faramineux volumes des transmissions. Le 10 septembre 2001, deux appels en provenance d'Afghanistan avaient été interceptés ; dans le premier, une voix annonçait : « Demain est le jour J », dans le second : « La grande partie est commencée » ; ces échanges n'avaient pas été signalés par les systèmes automatisés d'alerte. La volonté de saisir le plus grand volume de données appelle la mise en place de procédures toujours plus massives, qui portent dans leur gigantisme même une forme de limite technique et légale – du moins « jusqu'à nouvel ordre ». Trois opérateurs téléphoniques (regroupant à peu près 220 millions de clients) avaient accepté de remettre à l'agence les relevés de communications ; les conversations n'avaient pas été écoutées, mais des diagrammes dynamiques et précis des relations entre personnes avaient été élaborés. Les Américains ont appris par la presse que leurs conversations téléphoniques vers l'étranger étaient analysées mais également leurs communications domestiques, et ce sans autorisation judiciaire. Révélations qui ont scandalisé le pays et relancé le débat quant à l'équilibre à instaurer entre stratégies antiterroristes et protection de la vie privée des citoyens.

« Nous ne prenons pas le moindre risque avec le quatrième amendement de la Constitution » (garantissant la vie privée des personnes), affirmait en 1999, sous la forme d'une dénégation quasi explicite, Michael Hayden, général quatre étoiles de l'armée de l'air et directeur de la NSA. En 2002, un ordre présidentiel a concédé à l'agence un accès direct, illimité et sans aucun contrôle aux réseaux de télécommunications américains via des *trapdoors*

(portes cachées) dans les systèmes de commutation. La NSA identifie et détermine seule les numéros et adresses électroniques à surveiller et n'est pas tenue de solliciter une autorisation systématique du département de la Justice ou de la Maison-Blanche. Suite au 11 septembre 2001, les États-Unis ont ignoré les lois qui limitaient, depuis l'affaire des écoutes du Watergate, les activités des services de renseignement sur le sol américain, conformément à une priorité politique implicite désormais accordée au pouvoir exécutif, opérant une torsion sur les agencements démocratiques historiques au nom de l'impératif sécuritaire : « Le principe démocratique de la division des pouvoirs est aujourd'hui caduc ; le pouvoir exécutif a de fait absorbé au moins en partie le pouvoir législatif. Le Congrès n'est plus l'organe souverain auquel revient le pouvoir exclusif d'obliger les citoyens par la loi : il se limite à ratifier les décrets promulgués par le pouvoir exécutif¹. »

Le 24 octobre 2001 (soit six semaines après le 11 septembre), le Patriot Act, rédigé dans l'urgence, est voté au Congrès. Il autorise et facilite l'accès des services de police à des fichiers de toutes sortes (bancaires, commerciaux, professionnels, fournisseurs d'accès Internet, bibliothèques, hôpitaux...). Le FBI peut faire usage de « lettres de sécurité nationale » sans solliciter d'autorisation préalable ; toute personne visée par un tel mandat a interdiction d'en parler à quiconque, à la seule exception d'un avocat. « C'est dans la perspective de revendication des pouvoirs souverains du président dans une situation d'urgence qu'il faut considérer la décision du président Bush de se désigner constamment lui-même *Commander in chief of the army*. Si un tel titre implique une référence immédiate à l'état d'exception, Bush est en train de créer une situation où l'urgence est devenue la règle et où la distinction même entre la paix et la guerre (et entre guerre extérieure et guerre civile mondiale) devient impossible². » L'incertitude terroriste produit non seulement des déséquilibres entre les différents nœuds de pouvoirs démocratiques, mais favorise encore une propension fantasmatique à vouloir infiltrer l'ensemble des réseaux susceptibles de fournir des informations jugées utiles : « En septembre 2002, Washington demande à pouvoir consulter les fichiers informatiques des compagnies aériennes européennes afin de détecter les terroristes ayant réservé un vol pour les États-Unis. De longues négociations s'engagent avec Bruxelles³. » Le 5 janvier 2004, le programme *US-Visit* entre en vigueur, les photographies et empreintes digitales des ressortissants étrangers arrivant aux États-Unis sont saisies et archivées pour une période de soixante-quinze années, et iront se loger dans diverses bases de données des agences nationales de sécurité. La même année, le Conseil de l'Europe autorise les États-Unis à consulter les fichiers des compagnies aériennes européennes, en vue de repérer d'éventuels indices sur les listes de passagers voyageant à destination du territoire américain.

Gigantesques dispositifs légitimés par le spectre insaisissable des menaces qui requiert une vigilance *tous azimuts*, mais qui laissent apparaître

quotidiennement des failles, des dysfonctionnements, par la faute de mécanismes trop massifs, incapables de faire traiter correctement les magmas de données par des individus qualifiés ou des robots électroniques dédiés. La préparation de projets terroristes nécessite désormais d'éviter toute communication électronique au profit du contact direct ou de la transmission de signes non explicites mais suggestifs, toujours difficiles à interpréter. Obstacles qui conduisent le renseignement international – apte à modifier rapidement ses modes d'action – à envisager des *stratégies duales*, simultanément basées sur des systèmes automatisés et sur l'infiltration humaine, suivant une complexification des configurations susceptible d'amplifier davantage le principe d'une *suspicion indifférenciée* et généralisée des populations. Ces modes d'interception globale sont appelés à être moins systématiquement utilisés à l'avenir, au profit de l'analyse individualisée des comportements, non pas élaborée sur la captation de quelques registres d'activités identifiées mais sur le plus grand nombre d'actions quotidiennes – principalement commerciales et *professionnelles*. Amplification de l'observation des conduites, développée dans le cadre des activités salariées suivant un double objectif : à la fois opérer une pression psychologique sur le personnel et transmettre le cas échéant des informations à des instances étatiques de sécurité, tissant les filets d'une maille physique et virtuelle toujours plus informée et universelle.

Travail/évaluation

Les lieux de travail sont de plus en plus pénétrés par des systèmes d'observation intégrés. Les entreprises développent des procédés de pistage suivant des dispositions plus ou moins légales : écoute des conversations téléphoniques ; interception des courriers électroniques ; visualisation en temps réel d'écrans d'ordinateur via un poste de contrôle dédié ; capture des mots de passe ; installation sur les disques durs de logiciels espions (*spywares*) ; analyse des performances au moyen de claviers équipés de capteurs ; badges « intelligents » destinés à suivre les déplacements dans les espaces... Le site video-surveillance.net annonce sans trouble aucun : « Gagnez en efficacité : utilisez la vidéosurveillance pour gérer vos ressources humaines ! » Nous sommes entrés, indique la CNIL, dans l'« ère du contremaître virtuel », qui permet de « tout exploiter sans que le salarié en ait conscience » et d'établir le cas échéant « son profil professionnel, intellectuel ou psychologique ». Néanmoins, les bornes juridiques imposent d'informer préalablement les employés relativement aux protocoles mis en place. Les véhicules de fonction sont équipés de navigateurs GPS, permettant leur suivi en continu et la vérification en temps réel de l'adéquation des parcours, conformément aux plans arrêtés par les chefs d'équipe. L'introduction progressive d'émetteurs GPS dans les téléphones portables favorise la localisation de chaque personne en dehors même des zones d'activité ;

méthode qui oblige néanmoins à un accord préalable, ainsi qu'à l'usage d'un système de déconnexion temporaire. Corps réduits à des pixels sur des cartographies virtuelles, soumis à des calculs et protocoles d'alertes électroniques.

La surveillance contemporaine du milieu professionnel ne vise plus la vérification de l'affectation des agents à des postes fixés ainsi que la bonne réalisation des tâches, mais une *quantification robotisée* des opérations et des initiatives menées par chacun. Les *mesures automatisées de productivité* s'intègrent aux processus de travail : calcul du nombre de frappes sur le clavier ; estimation de la qualité de la « relation client » lors de dissection d'entretiens téléphoniques, par exemple, à l'aide de logiciels capables d'attribuer des notes et d'estimer la progression des téléopérateurs ; évaluation multicritères des cadres d'après des algorithmes réglés suivant des conclusions émises par des cabinets d'audit... Affaiblissement continu de la faculté de maintenir une part de ses gestes à l'abri du « regard », légitimé par les rapports de pouvoir que suppose la hiérarchie professionnelle, non plus matérialisés dans un contrôle visible et autoritaire, à l'instar des contremaîtres omniprésents dans *La Grève* (Eisenstein, 1924), mais dans une forme de *servitude indolore* et toujours plus *intériorisée*, produite par une *expertise numérique et individualisée* des actions menées au quotidien⁴.

Informations recueillies et traitées qui exercent *silencieusement* une forme de domination hypermoderne parce que discrète et sans rupture, supposée « soft » puisque ne se pratiquant plus à même le corps, mais dans une distance « cool », celle caractéristique des environnements professionnels *transparents* et climatisés du XXI^e siècle. Redoublement de la dimension supposée « immatérielle » des occupations en une surveillance à l'apparence tout autant fantasmatiquement « immatérielle », mais bien plus *intrusive* et *efficace* que toutes les autres dispositions coercitives historiques. De surcroît, ces masses de données sont susceptibles d'être agrégées à d'autres sources, complétant encore le tableau infiniment détaillé de chacun, analysé et *interprété* dans sa dimension – ou ses traces – multicouches : à la fois salarié, consommateur, voyageur, citoyen, patient, disséminant sans fin, délibérément ou à son insu, autant d'indices relatifs à ses *atouts* ou à ses *faiblesses* physiques autant que psychiques.

RFID : le monde animé des objets

Plus les mécanismes sophistiqués de surveillance se développent, plus ils visent l'élaboration de cartographies individualisées et dynamiques des singularités, ne cherchant plus seulement à définir les spécificités propres et évolutives de chaque être mais également à opérer le suivi dans l'espace et le temps des *choses*. L'introduction récente et expansive de composants électroniques à l'intérieur de quantité d'objets autorise désormais l'observation du rythme et des déplacements d'entités supposées jusque-là

inertes, devenues capables de signaler l'état de leurs « pulsations vitales », conformément à un monde gagné par un *animisme* d'esprit asiatique maintenant globalisé. Les puces fonctionnent grâce à la technologie de radio-identification (*radio-frequency identification* ou RFID) : étiquette intelligente dotée d'une mémoire logée dans un microprocesseur et d'une antenne miniature capable de communiquer les données par fréquences radio. Les tags passifs, privés de source d'énergie propre, sont activés par le champ électromagnétique généré par les appareils de lecture ; leur distance de communication reste limitée de quelques centimètres à quelques mètres. Les tags actifs disposent d'une batterie intégrée qui augmente leur portée jusqu'à quelques dizaines, voire quelques centaines de mètres. Tous deux émettent et reçoivent de l'information, et leur mémoire est modifiable à distance. Le microdispositif infiltre progressivement le « monde des choses » : emballages de produits alimentaires ou domestiques, appareils électroniques, vêtements, chaussures, livres, jouets...

L'objectif initial ambitionne de délaisser l'usage des codes-barres, nécessitant un contact par opération manuelle, au profit d'une saisie immédiate par capteur, autorisant de surcroît des fonctionnalités augmentées. Le procédé offre quantité d'applications au secteur de la distribution : suivi des commandes, gestion des stocks, vérification en temps réel de l'approvisionnement des rayons, lutte contre le vol, traçabilité des produits... Couplée à un capteur de température, une puce peut, par exemple, signaler d'éventuelles ruptures dans la chaîne du froid. Le contenu des chariots sera bientôt analysé par système de lecture intégré grâce aux ondes émises, se substituant à terme aux caissières de supermarché. Les entreprises de transport public optent progressivement pour le badge RFID appelé à remplacer le ticket à usage unique ; depuis 2006 en région parisienne, le passe sans contact Navigo se substitue à la Carte orange : chaque passager s'expose à un *traçage* de ses déplacements et à une mémorisation archivée de ses actes quotidiens, susceptibles, par exemple, de vérifier un alibi ou d'informer un dossier d'instruction judiciaire. Plus largement, la baisse régulière du prix des étiquettes concourt à leur expansion planétaire et à l'adoption d'applications multiples : identification des congressistes par le Parti communiste chinois, classement des coureurs du marathon de Berlin, gestion du bétail par les fermiers, repérage d'animaux domestiques en cas de disparition... Le système *Speed-Pass* mis en place par Exxon Mobil dans ses stations-service permet, au moyen d'un tag RFID plaqué contre la voiture, d'être reconnu par la pompe à essence et de pourvoir le véhicule sans avoir à régler à la caisse. Économie d'opérations, conformément à l'ambition d'instaurer un environnement global toujours plus *fluidifié*.

L'infiltration progressive de puces à l'intérieur des objets contribuera à soumettre *simultanément* et plus *amplement* les corps à des procédures de traçage. Surgissement d'une nouvelle *strate inédite* formée par la passion

humaine pour le contrôle, capable de suivre la situation physique de chaque chose (localisation, fréquences d'utilisation, usure, température...). Plus encore, il se développe de nouveaux *nœuds observationnels*, où les usages témoignent de comportements précisément détaillés et étendus dans le temps, le long de la pluralité d'activités déployées au quotidien. *Outils* devenus de véritables *prothèses* du corps, non plus selon la définition anthropologique d'André Leroi-Gourhan, ou philosophique de Jacques Derrida, mais mués en *instruments sensibles* de récoltes informationnelles *collés* aux pratiques de chaque individu. Une modalité complexe s'instaure, au sein de laquelle les humains ne s'observeront plus exclusivement les uns les autres, mais observeront en temps réel « la vie des choses », qui à leur tour « moucharderont » les humains et communiqueront également entre elles, développeront des luttes de pouvoir, se surveilleront ou neutraliseront certaines fonctions, suivant un nouvel « écosystème » fondé, à l'instar de son « modèle anthropomorphique », sur le conflit et l'ajustement appelés à régir les conditions dynamiques ou darwiniennes de son existence.

Le port par les individus d'instruments tagués et interconnectés renforcera la cartographie de leurs relations à l'occasion de rencontres physiques qui produiront des traces relatives à la *nature des liens* (ludiques, professionnels, amicaux, sexuels...). « Le Big Brother qu'Orwell craignait pourrait se matérialiser sous la forme de “Small Brothers” beaucoup plus sophistiqués⁵. » Et beaucoup plus *intégrés* que les « télécrans » de 1984, puisque extrêmement discrets ou quasi invisibles. Chaque objet devient émetteur ou récepteur d'information et acquiert le statut de chose unique, manifeste dans sa codification ou « ADN électronique », capable de communiquer avec d'autres appareils à l'intérieur d'une gigantesque maille au sein de laquelle un réfrigérateur, par exemple, sera capable d'informer de l'absence d'un produit un téléphone portable, qui lui-même pourra aussitôt passer commande auprès de robots électroniques, grâce au nouveau protocole global qui se met en place, capable de standardiser l'interrelation électronique entre entités matérielles, dédoublant la « Toile initiale » en un *Internet des objets*.

Un protocole nommé *Object Naming Service* (ONS) sera pour l'« Internet des objets » ce que le DNS est à l'Internet actuel, il permettra de relier entre eux des milliards de produits et machines en une sorte de « matrice seconde » destinée à administrer le système global de « vie », de circulation et de vérification, de la totalité des objets tagués de la planète. Phénomène d'amplification et d'intensification de l'*interconnexion globale* déjà évoquée plus haut, induisant une aggravation de nature exponentielle du pistage des êtres, et rapidement suivi par une filature robotisée des choses et des choses entre elles. Plutôt qu'un retournement de la surveillance des personnes par les machines – cauchemar illusoire et rétro-futuriste du contrôle des humains par les robots –, il apparaît davantage une *prolifération* entrecroisée de faisceaux spécifiques de surveillance composant un environnement innervé de systèmes de captations *protéiformes*, *intelligents* et à terme interopérables, au sein

d'une maille « multisources » caractérisée par l'absence progressive de « trous ». « Autrefois, dans les grandes périodes modernisatrices, on pensait qu'on maîtrisait les phénomènes techniques et qu'on avait par conséquent cet être qui internalisait l'ensemble des éléments ; aujourd'hui, nous savons que nous ne maîtrisons pas les créatures que nous produisons. D'où ce retour du souci et de la vigilance⁶. »

Une forme de parade, dit-on souvent, consisterait à imposer un « droit à la déconnexion », à pouvoir établir un « silence des puces », ce qui renvoie dans les faits à une forme d'ignorance à l'égard de la force intrusive et toujours plus *incontournable* des protocoles numériques. Il serait évidemment légitime de décider librement de désactiver certains dispositifs, mais l'espoir d'une telle licence correspond à une période historique dépassée, celle où la connectivité relevait d'un *choix* qui nécessitait une opération : la mise en réseau via les flux téléphoniques à l'œuvre jusqu'à la fin des années quatre-vingt-dix⁷. Aujourd'hui, un « halo universel » englobe nos déambulations, qui occasionnent réceptions ou émissions de signaux sans nécessiter au préalable un assentiment, mais sont seulement activées par la simple présence d'un corps – équipé de puces internes ou externes – au sein d'atmosphères partout rendues *sensibles* par la généralisation du « sans fil » et de capteurs *ad hoc*. La CNIL argue qu'une solution parmi d'autres consisterait à neutraliser la puce RFID une fois l'objet acheté, mais c'est d'abord oublier les fonctionnalités positives qui seront offertes par le tagage (par exemple, une chemise capable d'informer une machine à laver des conditions spécifiques de nettoyage que ses tissus requièrent ; à l'instar du téléphone portable qui offre simultanément usages appréciables et procédures de traçage). Ensuite, c'est encore omettre l'apparition massive à venir d'objets dont le fonctionnement et le « développement » ou l'« actualisation » seront indissociables de leur connexion, situant ce droit à la déconnexion comme un principe louable mais inopérant dans un monde où les choses seront non seulement *animées* mais rendues *évolutives* par leurs mises en réseau.

Lawrence Lessig, juriste et professeur à Stanford, affirme pour sa part qu'« il faut que les citoyens s'occupent en amont de ces technologies, avant qu'elles ne s'imposent de "l'extérieur" et qu'elles ne deviennent incontournables ». Position certes irréfutable qui appelle débats et consultations publiques, mais surtout qui devrait être prolongée par des *décisions légales*, fixant certaines limites indépassables. Horizon nécessaire, à l'aspiration probablement tout aussi naïve, dans la mesure où la vitesse qui imprime les recherches dégage des perspectives industrielles et économiques au pouvoir de croissance tel qu'il sera politiquement et socialement difficile de le freiner. « Pour généraliser, d'ici à 2010, l'utilisation de puces RFID sur 50 000 à 100 000 milliards d'objets de la vie quotidienne, un projet, dénommé "AUTO-ID" et coordonné par l'université américaine du MIT, rassemble six centres de recherche (américains, chinois, japonais, européen, australien) et

réunit 103 “sponsors” parmi lesquels les cinq plus grands groupes de la distribution⁸. » Forces d’innovation qui se soucient peu du « droit à la désactivation », mais qui au contraire cherchent à exploiter les potentialités offertes par l’interconnectivité globale, inscrivant chaque individu et chaque chose comme un « point de richesse » d’autant plus prometteur qu’il sera relié pour le « meilleur des mondes » à tous les autres, au sein d’un système universel d’échanges « fluidifiés », offrant une infinité de services « *on demand* », décidant néanmoins de procédures de quantification *approfondies* et *continues*.

Transhumanisme nanotechnologique

Si des microprocesseurs sont appelés à intégrer la plupart des unités matérielles de notre environnement, ils *s’incorporeront* bientôt aux tissus des organismes, situant tout individu comme une *puissance de signal multifonctions* indéfiniment transmise à flux tendus. Ce qui pouvait apparaître comme une hypothèse futuriste et improbable commence depuis peu à trouver les formes d’une réalisation effective. L’entreprise américaine Verichip a déjà mis au point une puce fondée sur la technologie RFID en perfectionnant un système existant destiné à marquer le bétail ou les animaux domestiques. En 2004, le *Verichip* « humain » a obtenu son autorisation de mise sur le marché, et cherche depuis à étendre ses champs d’application possibles. Le secteur médical entend capitaliser la potentialité offerte par la mise en relation entre puces et bases de données, capable d’informer immédiatement des antécédents d’un patient, quelle que soit sa capacité ou non à s’exprimer. Plusieurs disothèques proposent l’usage d’implants afin de bénéficier d’entrées prioritaires et de régler les consommations par scannage de la peau. D’autres entreprises investissent un marché virtuellement gigantesque et explorent de nouvelles fonctionnalités : suivi d’unités militaires d’élite, de personnes atteintes de la maladie d’Alzheimer ou d’enfants en vue de prévenir des enlèvements...

Une des fonctions majeures à venir consistera à les substituer à terme aux documents d’identité et cartes de crédit magnétiques, à l’intérieur d’un environnement global modifié par le repérage en continu des corps et de leurs actions dans l’espace et le temps, par omniprésence de capteurs connectés à des banques de données dédiées. L’introduction de composants électroniques dans les tissus biologiques constitue un *saut* décisif dans l’histoire ; à coup sûr représente-t-elle la forme la plus achevée et la plus parfaite du suivi – sans rupture et multitâches – des personnes. Un système intégral de récolte informationnelle favorisera pistage ininterrompu des déplacements, analyses des flux biotiques, traçages des relations professionnelles, amicales ou sexuelles (par communication entre puces mitoyennes), saisie de quantités d’opérations (achats, conversations, loisirs, lectures – via livres ou magazines équipés d’étiquettes RFID), conformément à un *halo* universel qui

enveloppera tout être, le rendant littéralement et en tous points *transparent*. Michael Dahan, professeur au Sapir Academic College en Israël, est particulièrement pessimiste : « Avant 2020, on implantera une puce RFID, ou équivalente, sur tous les nouveau-nés dans les pays industrialisés. Prévues pour fournir d'importantes données personnelles et médicales, ces puces pourront être utilisées pour le traçage et la surveillance⁹. »

L'accélération exponentielle de l'innovation technologique bousculera probablement un calendrier prédictif basé sur des constats actuels, et rendra bientôt concevable une *mondialisation systématisée de l'implant*, développant une nouvelle maille haute définition : l'« Internet des corps », communiquant avec son modèle précédent, l'« Internet des objets ». Chairs et choses connectées entre elles, à l'intérieur d'une *sphère* individualisée et interactive où chaque mouvement suscitera modulations lumineuses, hydrométriques, climatiques, suggestions de services ou d'objets, autant qu'une pénétration évolutive et extrêmement raffinée de la psychologie de chacun, dans un monde numérique non plus vécu et médiatisé au moyen d'interfaces physiques (claviers, téléphones, télécommandes...) mais par une communication *invisible* et infinie entre organismes vivants et environnements physiques et virtuels, produisant des *adéquations relationnelles* inédites entre personnes et milieux, réglées par la suprématie du paramétrage algorithmique.

Modification annoncée du statut supposé immuable du corps, conformément à l'idéal « post-humain » en partie réalisé qui voudrait que l'« identité naturelle » puisse être soumise à des modifications structurelles et fonctionnelles par *hybridation* de substances : une « bioélectronique » appelée encore à amplifier performances physiques, mentales et sensorielles. Déjà, quelques adeptes de la « philosophie transhumaniste » fabriquent artisanalement leurs biopuces et se sont baptisés *The Tagged*, « Les Étiquetés ». L'un d'eux, par exemple, affirme : « J'ai toujours été attiré par l'idée qu'un jour l'homme et la machine allaient fusionner, s'interpénétrer. Ce processus est déjà en cours, avec la multiplication des prothèses médicales de plus en plus perfectionnées¹⁰. » Rêve d'une *post-humanité* qui liquéfierait les classifications anthropologiques jusque-là perçues comme absolument indépassables, au profit d'une *indifférenciation* croissante entre êtres et machines, ou entre *existence* et *surveillance*, banalisée par un progressisme technoïde naïf ou une irresponsabilité éthique patente : « Il y a déjà beaucoup d'extensions informatiques que l'on peut placer dans notre corps et notre cerveau. Et nous finirons par considérer que c'est un excellent endroit pour les disposer¹¹. »

Les développements présents et à venir des nanotechnologies amplifieront ce phénomène d'*intégration* d'éléments atomiques artificiels dans les organes, appelés à *quantifier* la nature des flux et à transmettre en temps réel les

informations à des serveurs dédiés à une veille thérapeutique individualisée. Composants capables d'avertir des états émotifs, destinés à être analysés lors de passages de points de contrôle ou à l'occasion d'entretiens de tout ordre¹². Le corps, nous l'avons vu, constitue la dernière limite à coloniser, en vue de confondre être de chair et puissance électronique de signal, en une *unité* devenue indissociable, soumettant chacun à un traçage continu de ses déplacements, de ses actions, de ses états médicaux, indépendamment de toute *prothèse externe*. Stade annoncé et en quelque sorte ultime de la surveillance, qui ne chercherait plus à disséminer les dispositifs de contrôle, mais seulement à *collecter* sans fin les masses de données à l'intérieur d'une matrice achevée où les capacités d'analyse détermineront la puissance future d'interprétation de la psychologie des individus¹³. Disparition progressive des points d'observation situés à *distance* – dont notre époque découvrirait un pic de présence provisoire – au profit de systèmes de transmission et de réception *implantés* et *invisibles*. « Ce qui me préoccupe dans le développement des nanotechnologies, c'est que cela ajoute un élément de complexité au rapport qui existe entre le droit et la technologie informatique. Outre les caractéristiques de mondialisation et d'accélération constante de la technologie informatique, qui rendent le travail des juristes d'autant plus difficile que le droit est conditionné par l'exercice sur un territoire, et qu'il doit fixer des règles reposant sur la pérennité face à l'irréversibilité des phénomènes, les nanotechnologies lancent un défi supplémentaire : comment élaborer des normes adaptées face à un phénomène dont la première caractéristique est que ses applications ne peuvent pas être observées avec un microscope normal¹⁴ ? »

Un nouvel horizon anthropologique se dessine, déterminé par la manipulation de l'infiniment petit, qui imposera une fusion entre corps, nanoprocesseurs et environnements infiltrés de capteurs, formant une trame numérique universelle au sein de laquelle calculs et analyses conditionneront *autorisation* et réalisation de la quasi-totalité des opérations. Surveillance *insensible* des personnes et des choses, à l'intérieur d'*ambiances* désormais réglées ou *réglementées* par des algorithmes – composés à des fins sécuritaires, commerciales, thérapeutiques – destinés à faciliter ou non la circulation des individus dans l'espace et l'usage des objets dans le temps. Robotisation interactive et évaluation à flux tendus des existences, encore complexifiées par la passion universelle du *voyeurisme* et de l'*exhibitionnisme*, aujourd'hui hypertrophiés par quantité de protocoles technologiques adaptés. *Exposition* des événements intimes et aujourd'hui *partagés*, composant une *strate* décisive et expansive du diagramme de la surveillance du XXI^e siècle, à l'écart de figures pyramidales, marquée par une *prolifération* de structures *horizontales* d'observation et de suivi, inscrivant désormais chaque être comme un *agent* actif et *complice* de la matrice globale.

- 1- Giorgio Agamben, *État d'exception, Homo Sacer, op. cit.*, p. 35.
- 2- *Ibid.*, p. 41.
- 3- Jacques Henno, *Tous fichés...*, *op. cit.*, p. 83.
- 4- « D'après un article de Kenji Hall de *Business Week* : Nec a créé un laboratoire où ses salariés sont sous constante surveillance pour étudier l'émergence d'idées nouvelles [...] caméras de surveillance dans les bureaux et les salles de réunion, micros, capteurs RFID [...] enregistrent tout ce qui se passe afin d'aider l'entreprise à comprendre comment se développe l'innovation » (Françoise de Blomac et Thierry Rousselin, *Sous surveillance ! Démêler le mythe de la réalité*, Paris, Les Carnets de l'info, 2008, p. 183).
- 5- Michel Alberganti, *Sous l'œil des puces. La RFID et la démocratie, op. cit.*, p. 14.
- 6- Bruno Latour, *Un monde pluriel mais commun. Entretiens avec François Ewald*, Paris, Éditions de l'Aube, 2003, p. 37.
- 7- « L'important ce sera peut-être de créer des vacuoles de non-communication, des interrupteurs, pour échapper au contrôle » (Gilles Deleuze, *Pourparlers*, Paris, Éditions de Minuit, 1990, p. 244).
- 8- Cécile Calla et Stéphane Lauer, « Achetez, vous êtes surveillé... », *Le Monde*, 4 février 2007.
- 9- Cité par Michel Alberganti et Corinne Lesnes, « Nuages à l'horizon pour l'Internet de 2020 », *Le Monde*, 2 octobre 2006.
- 10- Yves Eudes, « Digital Boys », *Le Monde*, 11 avril 2006.
- 11- Ray Kurzweil, « La singularité approche », par Charles Muller, *Chronic'art*, n° 40, nov. 2007.
- 12- George Orwell avait déjà anticipé, sous une forme moins perfectionnée, un système d'évaluation sécuritaire des émotions : « Il posa son sous-main sur ses genoux et recula sa chaise pour se placer aussi loin que possible du télécran. Garder un visage impassible n'était pas difficile et avec un effort, on peut contrôler jusqu'au rythme de sa respiration. Mais on ne peut maîtriser les battements de son cœur et le télécran était assez sensible pour les relever » (1984, *op. cit.*, p. 109).
- 13- « Les voyageurs sont tenus de répondre à une série de questions générées par ordinateur, ajustées selon le pays d'origine, tandis qu'ils mettent leur main sur un capteur "biofeedback". L'appareil enregistre les réactions corporelles aux questions et détermine si l'individu est suspect » (Armand Mattelart, *La Globalisation de la surveillance. Aux origines de l'ordre sécuritaire*, Paris, La Découverte, 2007, p. 190).
- 14- Alex Türk, « La majorité des Français n'ont pas conscience qu'aujourd'hui leur sphère de vie privée est en cause », *chat modéré* par Jean-Marc Manach, www.lemonde.fr, 10 juillet 2007.

VII

HORIZONTALISATION DE LA SURVEILLANCE

Voyeurisme et exhibitionnisme généralisés

Familistère de Guise

Au milieu du XIX^e siècle, Jean-Baptiste-André Godin, un riche industriel « philanthrope », conçoit une cité ouvrière en partie inspirée des théories de Charles Fourier et du phalanstère, qui inaugure le mouvement de l'habitat social : le familistère de Guise, édifice imposant, envisagé comme un « palais pour ouvriers », composé d'une large cour carrée ouverte à la lumière solaire par une baie vitrée mais refermée sur elle-même par quatre corps de bâtiments semblables et joints, qui imposent une visibilité réciproque entre chaque habitation opposée. De surcroît, les balcons qui devancent les appartements permettent la circulation à l'intérieur de chaque étage sous forme de rues-galleries, autorisant une portée discrète et provisoire des regards sur les logements. Louable volonté d'offrir à une population laborieuse des conditions de vie fortifiées par une hygiène et un confort inédits, mais au sein d'un agencement qui oblige à une expérience collective de l'observation mutuelle et continue du voisinage : « Le fait principal de l'ordre et de la bonne conduite au Familistère, explique Godin, c'est que chacun y est à découvert. Ici la régulation du comportement se fait par la pression du regard¹. » Structure d'aménagement qui reprend à l'oblique certains principes d'un autre ordre de l'architecture communautaire, fondée sur l'omniprésence de la surveillance et la menace de la punition : la prison. « Ceux qui enfreignent le règlement du Familistère sont dénoncés par les autres, mis à l'amende. Et en cas de récidive, leurs noms s'affichent sur un tableau avec exposé de l'infraction². »

Les jeux d'attention induits par la mitoyenneté sont en quelque sorte consubstantiels de l'agglomération des habitats, qui densifie le contact entre les personnes, suscite le voyeurisme et diffuse dans l'inconscient collectif des lois castratrices non écrites. Au Japon, par exemple, marqué par le confucianisme, le contrôle de soi et des autres constitue une norme sociale. Les comités de quartier (*tonarigumi*) supposent une intériorisation partagée de

règles dont l'application est virtuellement soumise à une vérification commune. En outre, le commissariat local (*koban*) ainsi que les ilotiers établissent des listes précises des habitants suivant une grille où affectations et comportements sont répertoriés et examinés au yeux de tous, selon des codes prescriptifs explicites et implicites. L'observation mutuelle entre individus correspond à une dimension anthropologique en quelque sorte transhistorique, qui s'est plus ou moins développée selon les contextes, et qui a connu au sein de la « première urbanité », celle de la ville féodale, les conditions idéales de son épanouissement. « Strehler, avec son scénographe Luciano Damiani, avait repris les données de l'urbanisme vénitien qui dégage, au centre, une petite place bordée de maisons dont les fenêtres servent d'emplacements privilégiés pour la surveillance de proximité. Mais chez Goldoni, et Strehler le montre, elle entretient et anime constamment la socialité. *Il campiello*, où personne ne peut se protéger du regard extérieur, ne stagne pas ; il s'agite et se remue au rythme de cette surveillance mutuelle. Sa séduction provient de la réversibilité permanente des rapports, car ici, c'est son caractère propre, personne ne se trouve assigné à une posture immuable et, successivement, peut voir ou être vu. La redistribution des rôles interdit toute dichotomie définitive ou évaluation morale durable : nul plus fautif que l'autre, et chacun, à tour de rôle ! Réciprocité absolue. [...] Chez Goldoni, la surveillance de proximité reste une source de socialité, dépourvue de ces dangers et menaces habituellement associés à la surveillance reliée aux autorités politiques³. »

Formes de surveillance certes indissociables d'une vie communautaire apparemment « refrénée », mais certainement pas indolores, appelant sans fin l'acte potentiel de la *délation* et la conséquence de peines plus ou moins justifiées. « Machines coercitives mutualisées », capables de tourner à plein régime jusqu'à une certaine échelle qui se brise dans l'avènement de la grande ville marchande et bourgeoise du XIX^e siècle, qui distend les *liens* entre personnes, soumises à la cruauté d'existences fondées sur la compétition et non plus sur la complémentarité (Balzac, Hugo, Flaubert). Dilution des *identités* emblématique dans le Paris impersonnel et industriel de Baudelaire, celui de la « seconde urbanité » qui fait circuler des *foules anonymes* et fugitives que le poème « À une passante » tenterait vainement de distinguer : « Car j'ignore où tu fuis, tu ne sais où je vais⁴. » Saut dans une *multiplicité* insaisissable qui défait l'entourage immédiat de sa puissance normative, mais la délègue à un *tiers* institué : une nouvelle police technicisée et mieux infiltrée, autant qu'elle affranchit le citoyen moderne d'une priorité médiévale accordée aux corporations et à ses pratiques fixées, au profit d'une nouvelle singularité fondée sur la liberté de circuler et le droit à l'autonomie. « Partout où la densité de l'agglomération est en rapport avec son volume, les liens personnels sont rares et faibles : on perd plus facilement les autres de vue, même ceux qui vous entourent de très près et, dans la même mesure, on s'en désintéresse. Comme cette mutuelle indifférence a pour effet de relâcher la surveillance collective, la sphère d'action libre de chaque individu s'étend en

fait et, peu à peu, le fait devient un droit⁵. »

Troisième ville

L'urbanité contemporaine structurée de flux physiques et électroniques, innervée de connexions rhizomatiques locales et transnationales, soumise à déterritorialisation par des stratégies économiques multipôles ou des modes de vie nomades, à la fois désacralise le génie du lieu et fait de tout lieu l'occasion miraculeuse d'actions conduites à distance ou sans fil. Les espaces ne répondent plus à des types d'activités déterminés (emblématique dans le « zoning » moderniste) mais offrent l'occasion provisoire de constituer « sa propre sphère » de façon dynamique en privilégiant le *lien* au détriment des oripeaux *attachés* à la fonction. Quantité de protocoles interconnectés et miniaturisés maintiennent en continu des faisceaux relationnels entre individus, à tel point que la promiscuité caractéristique de la ville médiévale et classique se trouve aujourd'hui revitalisée, non plus par effets de proximité charnelle mais via les multiples canaux communicants ou à travers les « fenêtres digitales » ouvertes aux regards des autres. Réseaux et prothèses numériques transforment les comportements professionnels et sociaux et inaugurent une « troisième ville⁶ », caractérisée par un rapport élastique au territoire et l'instauration de liaisons indifférentes à toute attache locale. Surgissement d'une nouvelle « proximité à distance » qui, à la différence des modalités d'observation à l'œuvre dans la première urbanité, se constitue en partie par *consentement* à être vu et exposé aux « yeux anonymes du monde ».

Universalisation des dispositifs « embarqués » sur les corps⁷, destinés à émettre et recevoir textes, sons ou images, bref à communiquer multicanaux + multimédias, autant que machines à *exciter* exhibitionnisme et voyeurisme. La récente commercialisation de caméras pilotables et zoomables par IP (via Internet) induit une densification et une modification de la nature de la vidéosurveillance, non plus pointée par les institutions publiques ou privées vers les personnes, mais offerte aux individus désormais capables d'observer depuis leurs ordinateurs ou téléphones quantités de points situés jusque-là à l'abri (intérieurs des habitations, en vue de vérifier par exemple la bonne tenue de la nourrice, de la femme de ménage ou du conjoint...). Focales légères et peu onéreuses disposées aux abords des logements, équipées de détecteurs de mouvement destinés en cas d'intrusion à déclencher des systèmes d'alerte par SMS ou emails, offrant virtuellement à chaque citoyen doté des moyens financiers suffisants un appareillage policier connecté à des sociétés de surveillance *privées*⁸. Aggravation des jeux d'observation entre particuliers munis de moyens techniques et individualisés de contrôle social. « L'espace strié de la modernité construit un lieu perpétuellement livré et fondé sur un jeu dialectique avec son dehors. L'espace de la souveraineté impériale, par contre, est lisse. [...] Dans cet espace lisse de l'empire, il n'y a pas de lieu du pouvoir – il est à la fois partout et nulle part. L'Empire est une

u-topia, ou plutôt un non-lieu⁹. »

Mini-caméras également aptes à épier voisins, collègues, concubins..., ou mini-enregistreurs et autres « laisses électroniques » quasi invisibles infiltrant habitats domestiques ou espaces urbains, à l'instar des mini-appareils photo commandés à distance, nommés « *kozô* » au Japon, qui incitent à guetter les toilettes publiques ou les habitats des jeunes filles célibataires, produisant des images intimes et volées, souvent diffusées sur la Toile par de nouveaux « paparazzi masqués ». Amplification de la promiscuité classique qui ne s'opérerait qu'à travers les ouvertures des habitations, ici *pénétrées* dans leur profondeur privée. « Démocratisation de l'espionnage », par le fait d'un rapport à l'altérité prioritairement capté, calculé, localisé, suivi, archivé, instaurant un nouveau paradigme dans la relation à l'autre non plus médiatisée par la distance du regard – qu'il soit manifeste ou dissimulé – mais traitée par des codes et réglée par une *interface* technique, à l'intérieur d'une *télévidéosphère* intégrale puisque susceptible de saisir toute personne toujours située en théorie face à des viseurs – publics ou privés – omniprésents. « Robert Rimbaud, un DJ britannique, utilise un récepteur radio à longue portée, détourne, mixe et remixe les conversations qu'il attrape ainsi au vol sur des téléphones mobiles. Cet artiste, qui s'est choisi comme pseudonyme le nom de son appareil d'espion aux écoutes (sur ses disques, il signe Scanner), qualifie lui-même sa musique de “voyeuriste” et la décrit volontiers en usant d'une analogie filmique ; ainsi déclare-t-il : “Selon moi, scanner des sons est comparable à cartographier une ville. La séquence d'ouverture de *Short Cuts*, film de Robert Altman, donne une représentation assez juste de mon travail : la caméra survole la ville et, à mesure qu'elle parcourt l'espace, on entend les conversations des habitants”¹⁰. » Jennifer Ringley, jeune femme américaine, qui dans les années quatre-vingt-dix fut une des premières à « déflorer » en continu sa vie domestique et sexuelle au moyen de webcams disséminées dans son logement, annonçait d'une façon systématisée et emblématique la nouvelle aptitude contemporaine à se défaire de sa vie privée, à l'exhiber, ou à pouvoir y assister grâce au pouvoir du Web. Jennicam inaugurerait *visiblement* une structure relationnelle *ubiquitaire* et globale, déterminée par l'infiltration et la connexion de circuits vidéo au sein des surfaces privées et publiques de la planète, assignés à exposer sans limite spatiale ou temporelle une infinité d'événements plus ou moins volés et mondialement *partagés*.

Reality shows

Le Diabolique Docteur Mabuse (Fritz Lang, 1960) déploie un dispositif situé à l'intérieur d'un grand hôtel berlinois, composé de glaces sans tain et de nombreuses caméras reliées à une régie qui autorise contrôle et voyeurisme, autant par les membres de la direction que par certains clients. Peut-être ce film a-t-il inspiré l'imaginaire aux aguets des producteurs de télévision

américains, qui dans la décennie suivante cherchaient à inventer de nouvelles formes davantage dramatisées et aux pouvoirs de projection intensifiés. Enjeu de l'admirable *Network* de Sydney Lumet (1976), manifeste dans l'hystérie du personnage joué par Faye Dunaway, dont la fonction consiste à concevoir les programmes les plus poignants et spectaculaires possibles. Car bien avant la diffusion *live* d'événements intimes visibles en ligne, les vocables de *reality show* ou de *real TV* étaient apparus dès le début des années soixante-dix. Un prototype intitulé *An American Family*, diffusé aux États-Unis en 1973, consistait à introduire une équipe de réalisation dans un habitat privé et à filmer pour la première fois *de l'intérieur* une famille californienne en crise jusqu'à son « dénouement » : le divorce des parents. Le principe fut repris l'année suivante en Grande-Bretagne, sous le titre *Family*. En 1987, une quarantaine d'émissions de *télé-réalité* furent produites et rencontrèrent de fortes audiences. C'est au cours de la décennie suivante que le format connut une expansion mondiale : *Big Brother*, imaginé par la société néerlandaise Endemol, exposait douze personnes cloîtrées dans un espace commun, de toutes parts saisies par un circuit vidéo interne. Leurs activités quotidiennes étaient diffusées en quasi continu et excitaient curiosité et voyeurisme du public. Les taux d'audimat rencontrèrent une telle audience que le « concept » a été exporté et repris par soixante-dix chaînes dans le monde, notamment présenté en France sous le nom de *Loft Story*, dont le succès a inauguré pour une bonne dizaine d'années la généralisation de la télé-réalité. Expérience collective et exaltée de la visibilité la plus banale et la plus intime de personnes soumises à une « nudité télévisuelle ».

Dans un épisode de la série *Desperate Housewives*, une femme visionne tous les soirs, de retour chez elle, les activités de la nounou et de ses enfants grâce aux images saisies par une mini-caméra dissimulée dans son logement. Dispositif télévisuel spéculaire dans lequel une fiction *représente* une *télesurveillance* individualisée autant qu'elle *enregistre dans la réalité* le statut désormais généralisé de chaque *télespectateur* ou témoin *anonyme* d'événements tout aussi privés mais publiquement *broadcastés*. Le film *The Truman Show* (Peter Weir, 1998) cristalliserait en quelque sorte le comble d'un voyeurisme impitoyable et communément partagé : un homme joué par Jim Carrey, adopté dès sa naissance par une société de production, ignore arpenter une réalité fictionnelle entièrement composée de comédiens qui l'environnent. Vie singulière continuellement soumise à une *pénétration publique*, qui sacrifie un être sur l'autel d'une passion collective, et dont la radicalité des moyens mis en œuvre se retournera *in fine* contre l'équipe de réalisation, qui assistera impuissante à l'affranchissement de Truman, sous les vivats de télespectateurs schizophrènes, à la fois ravis de sa libération mais bientôt orphelins de leur show quotidien. Duplicité universelle qui mêle dans une même pathologie globale une appétence pour l'observation des autres autant que sa condamnation quasi unanime.

Repérages « à la demande »

La société japonaise NTT fut la première à proposer un service de localisation de proches, notamment d'enfants, sous le nom de *Imadoko* (« Où es-tu ? »), grâce à une puce intégrée dans le téléphone portable permettant le suivi et la visualisation des déplacements sur une carte géographique dynamique accessible en ligne. L'opérateur téléphonique allemand T-Mobile commercialise également un système de positionnement par satellites qui peut être exploité par une tierce personne sur son propre mobile, sous réserve du consentement de l'utilisateur tracé. Modalité relationnelle instaurée avec son entourage, qui exclut désormais la licence du vide et la part d'ignoré qui fonde le rapport à l'autre, suivant le principe éthique d'une confiance nécessairement inquiète mais consubstantielle du *lien à distance* entre les individus, au profit d'un *repérage* robotisé des déambulations du corps. À l'avenir, la *nature* même des activités sera probablement rendue transparente, annulant définitivement la dimension propre, intime, de tout être, devenu surface de visibilité ininterrompue et *mutuellement partagée*. On sent que pointe ici une autre rupture d'ordre anthropologique, qui voit la notion moderne d'*intersubjectivité* appelée à se dissoudre dans celle d'*interpénétration électronique réciproque*.

Une société britannique, Blade Runner, conçoit des vêtements pour enfants équipés d'un capteur GPS prioritairement destiné à les localiser et à connaître l'historique de leurs mouvements lors des derniers mois. En outre, le franchissement d'un périmètre non autorisé déclenche un signal SMS transmis aux parents, qui institue dans les relations des contraintes physiques prescriptives robotisées inédites, à l'intérieur d'un *néopanoptisme sans fil* virtuellement intégral. Dispositif à l'œuvre dans le *bracelet électronique*, supposé favoriser l'avènement de la nouvelle prison « immatérielle » du XXI^e siècle, dont le principe structure déjà plusieurs modes de surveillance spécifiques : « bijoux » électroniques pour les nouveau-nés et pour les patients atteints de la maladie d'Alzheimer ; capteurs de mouvement ou de température placés au domicile de personnes âgées ; protocoles d'alerte à l'intention d'individus handicapés... Substitution progressive de « solutions » techniques au détriment de comportements de proximité fondés sur la vigilance et la chaleur de la présence charnelle, induisant *distance* et déresponsabilisation possible des membres familiaux, des personnels soignants, des assistants sociaux..., au profit d'une priorité déléguée au *signal d'alarme électronique*.

Jill Starishevsky, une procureure new-yorkaise, a récemment mis au point un site intitulé HowsMyNanny.com, qui permet de suivre par GPS les déambulations des nourrices et des enfants. Une plaque d'immatriculation fixée sur la poussette indique également l'adresse Internet. Les parents peuvent non seulement vérifier les déplacements, mais également être avertis

de conduites jugées « inappropriées » par des passants gardant leur anonymat et transmettant les coordonnées au site qui enverra aussitôt emails ou SMS d'alerte. *Horizontalisation* d'une partie des faisceaux observationnels, dont la densité appelle *de facto* nombre d'entre eux à devenir indissociables de *dénonciations* ou de *délations* publiques et *masquées*. La société Overspy propose contre un abonnement mensuel de soixante-dix euros le transfert de courriers électroniques envoyés ou reçus par son conjoint, par exemple, ainsi que la liste des sites visités au jour le jour. Un logiciel fourni par la compagnie Pipistrel permet de récupérer sur son propre téléphone les textos rédigés ou réceptionnés par une tierce personne. Infiltration de dispositifs d'espionnage invisibles, susceptibles de « modérer » les rapports entre couples et d'interdire encore toute « part secrète » pour une transparence standardisée et tendanciellement permanente.

Il se constitue progressivement un inquiétant « esprit du temps », marqué par une généralisation multiforme de la *suspicion* à l'égard des pouvoirs politiques, des responsables économiques, des organes de presse. Nouvelles paranoïas notamment entretenues par les effets de « déhiérarchisation » des systèmes de structuration de l'information prioritairement induits par Internet, et qui redoublent le principe de *défiance indifférenciée* déployé dans les nouveaux paradigmes sécuritaires, que nous avons déjà examinés suivant cette mesure-là. *Méfiance* qui semble surnoisement gagner les rapports entre individus, favorisée par l'élaboration de techniques destinées à découvrir les « arrière-mondes » de chacun. Un test récemment mis au point et à l'attention de *tous*, nommé *Checkmate*, permet, à la vue d'une tache suspecte sur une culotte ou un bout de dentelle, de plonger le vêtement dans une solution qui révélera ou non la présence de traces de sperme. Dangereuse suspicion apte à façonner les *liens* fondés sur la *vérification* préalable et continue, au détriment de la « logique du soupçon » nietzschéenne, qui appellerait à se méfier d'une psychose collective autant formée par des structures culturelles apeurées que par des techniques qui cherchent sans fin à l'exciter davantage.

Tous témoins

Le tsunami qui a frappé les côtes de l'Asie du Sud en décembre 2004 a inauguré une nouvelle ère médiatique marquée par l'universalisation potentielle de chacun en témoin d'événements aptes à être saisis et aussitôt diffusés sur les sites de partage vidéo en ligne ou par les télévisions de la planète, qui *enregistrent* le statut inédit de toute personne désormais susceptible de remplir la fonction d'« agent de presse occasionnel » ou de capteur d'une réalité contemporaine quadrillée multigrilles par le fait de corps équipés de prothèses numériques. La globalisation quasi achevée du port de téléphones multifonctions, autorisant prise de photos ou d'images animées ainsi que leur transmission instantanée, modifie d'une part la nature historique du « reporter », envisagé comme la figure *assignée* à aller *au-devant* des faits

et à les rendre dans un second temps publics, et d'autre part la qualité du « regard ordinaire » en tant que faculté virtuelle d'assister par sa simple présence au surgissement imprévu d'événements et de les exposer suivant une portée *intégrale* en quasi-temps réel. Plusieurs sites Internet, notamment les deux plus importants, CitizenSide et YouWitness, réceptionnent, rémunèrent et mettent en ligne les images recouvrant valeur d'actualité au même titre que celles visibles dans le cadre d'un journal télévisé, mais avec la différence qu'elles ne sont surprises que par des personnes devenues pour un moment les témoins privilégiés d'une scène méritant une exposition publique.

Glissement progressif de la place de l'individu compris comme un être fuyant, et *de facto* insituable par sa faculté de mobilité, vers celle de *témoin disposé* le long d'un continuum théoriquement ininterrompu et refermant dans sa *multitude anonyme* la sphère d'une visibilité maintenant *globale*. Évoquant plus haut les attentats commis à Londres en juillet 2005, nous avons signalé avec quelle mesure les images de télésurveillance de la ville avaient été visionnées ; *simultanément*, les policiers londoniens avaient lancé un *appel à témoins* à l'attention de particuliers qui auraient saisi quelques images des terroristes ou des événements, inaugurant le surgissement irrémédiable d'une nouvelle *couche* d'yeux disséminés dans une réalité de toutes parts infiltrée de capteurs fixes ou mobiles, dont les différents régimes et pouvoirs se *relaient* suivant une panoscopie à focales variables mais à portée intégrale. Jacques Derrida avait exploré certains enjeux philosophiques induits par la figure du *témoin*, révélateur dans son statut fragile et hasardeux des « trous » et « manques » qui ponctuent les rapports spatio-temporels entre les êtres, interdisant toute vision totalisante et assurée du cours des choses. Le *témoin équipé* du XXI^e siècle inverserait ce symptôme, en annulant la possibilité de brisure qui toujours menace la *représentation* des événements épars dans leur soudaineté, et viendrait compléter dans sa foulditude, muni de ses prothèses miniaturisées et portables, les points jusque-là laissés plus ou moins vacants au sein de la matrice intégrale désormais ultra-densifiée, presque achevée, pourrait-on dire, à la nuance près que la virtualité du vide demeure, mais selon des taux de probabilité qui assurément se réduisent.

La fonction de témoin ne répond pas à un objectif unique ; le témoin indique *a posteriori* ce à quoi il a assisté, tout comme il peut signaler des faits qui sans lui seraient restés masqués, suivant une conduite susceptible d'informer heureusement une instruction aussi bien que de conduire à une dénonciation douteuse ou à une délation en cas de motif non fondé. Mission accidentelle qui nécessite une forme de conscience éthique, ou qui peut au contraire être excitée par le ressentiment et l'envie, ou l'illusion malsaine de participer individuellement et activement à l'ordre commun, situant chacun comme un « shérif potentiel » plus ou moins vertueux. La police du Var a expérimenté, en 2008, un système de réception de documents électroniques via une adresse email¹¹ où transmettre dénonciations écrites, photographies ou

fichiers vidéo d'images de délits saisies à la volée. Protocole discret mais qui *généralise* et institue non seulement la licence de l'*anonymat* – susceptible d'attiser consciemment ou inconsciemment mauvaise foi ou excès –, mais qui encore *délègue* au sein d'un nouveau type de socialité certains pouvoirs de police (dont la mission première consiste d'abord à *constater*, avant même que de les prévenir, les infractions à la loi) à toute personne dotée de prothèses électroniques connectées¹². La délation constitue, dans 1984, un acte civique, appelé à renforcer sans fin le pouvoir de Big Brother ; le *témoignage électronique et anonyme*, lui, intensifie presque sans trace visible la *dimension participative* d'une citoyenneté non plus envisagée comme une distribution organique et pourtant structurée, parfois *assermentée*, des missions de chacun, mais comme un ensemble à *responsabilité collective*, tendanciellement indifférenciée et illimitée par des systèmes techniques mutualisés aux incidences juridiques et sociales complexes, néanmoins mis *à la disposition de tous* sans aucune expertise éthique et qualitative ou concertation législative préalable¹³.

Un renversement s'est récemment produit, principalement aux États-Unis, sous le vocable de *copwatching*, qui consiste à soumettre légalement les activités des forces de police à l'observation régulière d'équipes de bénévoles appelés à assister et à filmer conversations entre policiers et citoyens lors de rondes ou d'arrestations. L'enjeu étant de *constater* les excès ou manquements à la loi et de les diffuser le cas échéant sur Internet ou de transmettre les documents aux chaînes de télévision. Retournement qui recouvre peut-être une valeur salubre, mais qui dans le même mouvement intensifie le principe de *suspicion généralisée*, n'épargnant aucun corps individuel ou collectif, conformément à de nouvelles structures multifaisceaux à *dimension spéculaire*. Suivant une visée déclarée qui cherche à parfaire une mise à plat normative, coercitive et *réciproque*, à éviter le trou, la fameuse « case vide » conceptualisée par Deleuze, qui évoque la force vitale et ludique induite par le franchissement ou l'*affranchissement* du miroir par Alice, dans son pays des merveilles, à l'opposé de nos consciences toujours plus refermées *entre elles-mêmes* ou *verrouillées* par leur interconnexion mutuelle.

Identités individuelles mises à nu par le Web même

Le principe d'une cartographie standardisée, dynamique et individualisée des personnes a éclos en une durée très courte au regard d'une prétendue linéarité historique, à la vitesse de la lumière en quelque sorte, notamment par l'usage de bases de données structurées et offertes à tous, sous le nom de *moteur de recherche*. Outre le fait que quantité de types de requêtes hétérogènes sont permis, une prééminence portée sur les noms propres s'est symboliquement imposée, qui a rendu possible l'accès à des informations relatives à Napoléon ou à Orson Welles autant qu'à un voisin ou à une personne tout juste rencontrée. Google, le premier d'entre eux, n'a jamais

demandé l'accord de quiconque afin d'aller rechercher les différents sites relatifs aux activités d'un individu, alors qu'il se produit dans les faits et le droit une visibilité publique de paroles et de gestes, sans aucun consentement déclaré. Exemplification des récents *panoptismes horizontaux* qui exposent librement et sans frontières toutes sortes de renseignements, désormais perçus comme un acquis inaliénable, encouragé par le fantasme triomphant d'une transparence globale aux vertus censées offrir un « surcroît démocratique ». Certains moteurs se sont spécialisés dans l'inspection des identités individuelles, à l'instar de Spock (acronyme de « Single point of contact and knowledge ») qui produit des fiches informatives supposées plus précises et dénuées d'erreurs, notamment à l'égard des homonymies, et susceptibles d'être consultées par des employeurs potentiels, par exemple, suivant une mise à plat informée et accessible des antériorités et pratiques des personnes.

L'ambition d'exposition universelle des corps et des conduites, développée tous azimuts par Google, a conduit la compagnie californienne à démultiplier les formats techniques de visibilité – ceux-ci davantage consentis. L'Agenda Google (*Google Calendar*) permet de partager une partie ou l'intégralité de son emploi du temps avec d'autres utilisateurs. Les fichiers des ordinateurs sont visités et indexés par *Google Desktop*, rendus disponibles en ligne, si l'utilisateur le souhaite, grâce à *Google Documents*. Quant au dispositif *Google Health*, il expose les dossiers médicaux complets en ligne, à l'attention de médecins ou d'organismes de santé, non seulement soumis au risque d'infiltrations mais contribuant surtout à *externaliser* une part de l'*intimité psychophysiologique* de l'individu, située à l'abri depuis l'Antiquité grecque d'Hippocrate, et glissant irrémédiablement vers la notion de *profil thérapeutique partagé*, aux fonctionnalités peut-être *augmentées*, mais opérant une torsion sur la *relation frontale sauvegardée* par le secret médical qui règle le pacte historique et exclusif entre le praticien et son patient.

Ce qui est nommé « Web 2.0 », « web communautaire » ou encore « réseaux sociaux » (*social networks*) constitue un mégasystème protéiforme de cartographie dynamique des identités, des activités et des *relations* entre individus, non plus révélées par des conduites observationnelles menées par des entités publiques ou privées, mais édifiées *volontairement* dans une sorte d'excitation collective à divulguer sa vie aux yeux de tous. Les individus sont alors *reliés* par un sentiment d'appartenance mutuelle et complice à une même « sphère d'intérêt », conditionnant un nouveau paradigme relationnel *formaté* et universalisé, superposant dans un même mouvement *exhibitionnisme* et *voyeurisme*. Quantité de sites parmi les plus fréquentés contribuent à intensifier ce *dévoilement* à la fois individualisé et planétaire : gestes relatés, photographiés, vidéographiés, suivant des styles « trash », « néopop » ou à l'allure plus sobre, sur MySpace, Facebook, LinkedIn, Orkut, Friendster, ou le chinois QQ.com (classé au cinquième rang des visites mondiales) ; possibilité de retrouver ses amis d'enfance ou d'adolescence sur « Copains d'avant » et

ses nombreux équivalents, qui informent notamment des parcours scolaires et universitaires ou qui affichent les CV ; sites plus spécialisés tels Cyworld, Mixi, ou le Home de Sony à l'attention des « videogamers »... En outre, la prolifération de blogs amplifie sous d'autres formes la publication de pensées, d'opinions à l'intérieur d'une maille globale où chaque individu estime désormais avoir gagné le droit d'obtenir des informations à l'égard d'autrui autant que de concéder librement une mise à nu de soi.

La durée d'archivage des données ainsi que la demande, souvent compliquée et incertaine, de destruction des informations constituent un enjeu juridique présent et à venir d'importance, dans la mesure où s'instaure une « fixité des identités » en double contradiction avec le devenir de l'existence et la dimension dynamique et sans cesse évolutive du Web. La mémoire astronomique de la Toile et de ses outils d'indexation représente une puissance d'auscultation des personnes d'après une *profondeur historique* toujours plus ample, dont les usages postérieurs des traces par des tiers peuvent se retourner contre leurs auteurs, et qui appellent des modalités d'utilisation (et d'effacement) justement réglementées, et des encadrements juridiques aptes à protéger le droit fondamental à la *prescription* ou à l'« oubli ».

Une sorte de comble de visibilité publique des identités encore entremêlées à une dimension délatrice se cristallise dans le site américain Intelius.com, qui permet d'accéder sous réserve d'abonnement mensuel à la fiche hautement détaillée de personnes de son entourage : voisins, nourrice, futur gendre ou employé... Quantité d'informations hétérogènes sont accessibles : situation familiale, niveau de revenu, patrimoine, type d'habitation, degré d'éducation, sensibilités spirituelles, affiliations politiques... La compagnie prétend divulguer légalement « la vérité sur chacun d'entre nous », conformément à ce souci névrotique contemporain de transparence généralisée, aux effets sociaux supposés recouvrir des vertus coercitives et « prophylactiques ». Les registres se constituent grâce à la récolte sophistiquée et structurée des flux de données disséminées par chacun : achats à des sites spécialisés, commandes en ligne, abonnements aux journaux et magazines, historiques scolaires et universitaires, cadastres immobiliers, rédaction de blogs... Un autre échelon, moyennant un surcoût financier, propose de consulter les casiers judiciaires, grâce à la publication des arrêts de cours de justice ainsi que l'accès aux archives. Le site Familiwatchdog représente un palier supplémentaire dans la pénétration intime des antécédents d'autrui, mais davantage « spécialisé », dans l'*exposition* en toute légalité des profils de personnes ayant commis des exactions sexuelles. Auscultation universelle et accessible des identités, constituée par agrégations de contributions administratives et individuelles.

Un autre principe d'horizontalisation dans la *visibilité partagée* des personnes consiste à renforcer la *mutualisation* des informations, sous la

forme d'une *évaluation réciproque* des gestes et des performances produits par l'altérité planétaire. Une tendance récemment apparue cherche à instituer un principe d'estimation formulée par les usagers à l'égard de certains membres d'une corporation, professeurs ou médecins par exemple, sous la forme d'un commentaire subjectif et d'une *notation*. Le site Note2be.com – au slogan explicite : « Note ton professeur ! » – encourage écoliers et lycéens à émettre des appréciations à l'égard de leurs enseignants, à la fois supposées offrir des outils d'information destinés aux parents et entendues comme une sorte de « droit à la réciprocité » confirmée par une phrase de Sartre visible sur la page d'accueil qui énonce : « Tout est là : si celui qui juge n'est pas lui-même jugé, il n'y a pas de vraie liberté. [...] Cela suppose que chaque enseignant accepte d'être jugé et contesté par ceux auxquels il enseigne, qu'il se dise : "Ils me voient tout nu." » (Jean-Paul Sartre, *Le Nouvel Observateur*, 19 juin 1968). Est-il nécessaire de signaler d'abord que cette assertion, outre qu'elle n'a aucune valeur de vérité, a été prononcée le mois suivant les événements de mai 1968, mais surtout que le principe opère une *confusion* infondée entre des fonctions *irréductibles*. La position d'élève renvoie à un âge et à un besoin d'apprentissage ; celle de pédagogue, à une fonction et à une mission professionnelles.

Le souhait d'une *mise en regard analogue* non seulement relève d'une absurdité conceptuelle, mais révèle en creux un des symptômes de notre temps : celui qui vise à situer tout individu comme un juge potentiel et *actif* des gestes d'autrui, à l'écart des principes démocratiques qui instituent le pouvoir de *délégation* et de *compétence spécifique* reconnue et sanctionnée par des diplômes et une aptitude validée. Le projet de « jurys populaires » ou de « tribunaux citoyens » émis par Ségolène Royal lors de la campagne de l'élection présidentielle de 2007 répond exactement à cette névrose collective simultanément fondée sur un sentiment de *suspicion* généralisée appelé à être maintenu sans fin, et sur l'illusion d'imaginer chacun, au nom de l'égalité républicaine, comme bénéficiant *de facto* d'un autre type d'égalité, non pas seulement celui légitime d'avoir une opinion subjective et publiquement exprimable, mais d'être doté depuis peu d'un droit et d'une aptitude à *expertiser* qui que ce soit. Dissolution des différences qualitatives entre individus au profit d'une *veille mutualisée* et *collaborative* entre les êtres. Structure sociale qui correspond exactement aux schémas relationnels à l'œuvre dans 1984 d'Orwell, mais qui ici trouve sa légitimation dans une nouvelle « liberté d'expression » exaltée par la transparence inédite offerte par le Web *participatif*.

D'autres catégories de sites aux ambitions similaires, Note2bib.com ou demedica.com, proposent de soumettre son médecin à un examen radiographique, d'après plusieurs paramètres commentés et notés : hygiène, confort, temps d'attente, comportement... Une aggravation de la vigilance collective trouve une sorte d'achèvement factuel et symbolique dans le nouveau concept managérial d'*auto-évaluation*, qui consiste à enregistrer par

exemple ses propres conversations téléphoniques et à les exposer à évaluation en compagnie de collègues ou de cadres. Technique de « montée en compétences », ou « outil de coaching », opérant une confession destinée à favoriser un perfectionnement continu grâce à des procédés simultanément fondés sur la « libre » auscultation minutieuse de l'autre, et sur son envers culpabilisé éventuellement objet de sanctions : une *autocritique* soumise à *pénétration publique*.

La multiplicité et la variété des *faisceaux horizontaux d'observation* composent non seulement une autre strate protéiforme au sein de la matrice globale mais, à la différence des autres couches que nous avons jusqu'ici explorées, ne constituent pas une modalité supplémentaire : elles *redoublent* l'ensemble en un *autopanoptisme électronique universel*. Appropriation individualisée et techniquement possible de la quasi-totalité des protocoles de traçage, qui vient se superposer en milliards d'unités ou d'individus à des procédés de suivi gérés par des entités publiques et privées. Dimension « ultracomposite », organique et mobile de la surveillance contemporaine, qui ne forme pas une notion ou une configuration homogène, qui ne se loge dans aucun système unifié, mais qui se tisse de façon dynamique par le foisonnement d'yeux et de capteurs humains ou électroniques en réseaux *épars* ; abyssale complexité rétive à toute solution exclusive appelée *plus que jamais* à faire l'objet d'une *infinité* d'*ajustements* sociaux, politiques et juridiques, d'initiative locale ou globale, individuelle ou collective.

1- *Le Familistère de Guise, une cité radieuse au XIX^e siècle*, film de Catherine Adda, collection « Architectures », Arte vidéo, 2001.

2- *Ibid.*

3- Georges Banu, *La Scène surveillée*, *op. cit.*, p. 39.

4- Charles Baudelaire, « À une passante », *Les Fleurs du mal*, 1857.

5- Émile Durkheim, *De la division du travail social*, Paris, PUF, « Quadrige », p. 286.

6- Cf. Dominique Boulier, *La Troisième Ville*, Paris, L'Harmattan, 2000.

7- En 2006, le cabinet IDC a estimé à plus d'un milliard le nombre d'appareils capables de saisir photos ou vidéos ; ce volume ne cesse de s'accroître.

8- Cf. le phénomène planétaire des *gated communities* ; sur les questions de la privatisation de la sécurisation des habitats, je renvoie au livre de Mike Davis, *City of Quartz. Los Angeles capitale du futur*, Paris, La Découverte, 2006 ; à celui de Stéphane Degoutin, *Prisonniers volontaires du rêve américain*, Paris, Éditions de La Villette, 2006 ; et à l'ouvrage historique d'Evan McKenzie : *Privatopia : Homeowner Associations and the Rise of Residential Private Government*, Yale University Press, 1996.

9- Gilles Deleuze, *Pourparlers*, *op. cit.*, p. 219.

10- Peter Szendy, *Sur écoute, esthétique de l'espionnage*, Paris, Éditions de Minuit, 2007, p. 62.

11- police.83@interieur.gouv.fr.

12- « Après le 11 septembre 2001, le FBI a utilisé moult émissions de télé et de radio pour inciter chaque Américain à dénoncer "tout comportement suspect de la part d'amis, de proches, de connaissances et d'étrangers" ». Le gouvernement a été entendu puisque 700 000 voisins, petits commerçants et employés ont fait l'objet de dénonciations, en à peine deux mois

jusqu'à fin novembre 2001 » (Ariel Kyrrou, *Paranofictions. Traité de savoir-vivre pour une époque de science-fiction*, Paris, Climats/Flammarion, 2007, p. 63).

13- « Le *neighborhood watch*, ou surveillance de voisinage, fort de plus de 5 500 associations de quartier de surveillance du crime, est la plus importante contribution du LAPD à l'aménagement policier du territoire. [...] Un immense réseau de voisins attentifs participe d'un système de sécurité. [...] Aiguillonnés par le capitaine du quartier, les résidents deviennent plus vigilants dans la protection des propriétés et du bien-être de chacun. Ils communiquent immédiatement les comportements suspects » (Mike Davis, *Au-delà de Blade Runner. Los Angeles et l'imagination du désastre*, Paris, Allia, 2006, p. 68-70).

DISCOURS DE LA SERVITUDE VOLONTAIRE

(SUITE ET FIN ?)

Hong Kong la nuit sous la pluie. Dans une rue, quantité de parapluies ouverts et vus de haut empêchent d'apercevoir les visages de pickpockets rivaux fondus dans la foule. Image à la plastique insolite presque entièrement recouverte de noir et dont on comprend qu'en dessous, une menace virtuelle et continue enveloppe les rapports entre les passants plus ou moins épiés et susceptibles de dérober ou d'être dérobés. Scène finale du film *Sparrow* de Johnnie To (2008), emblématique d'un environnement contemporain caractérisé par une forme d'indolence ou d'ignorance à l'égard de pratiques camouflées et à la fois marqué par une structure de part en part *paranoïaque*. Aucune privation de droit ici, mais davantage un ensemble formé de jeux d'observation tendanciellement anonymes au sein duquel chacun cherche en puissance à fixer la valeur de chacun ou est susceptible d'être soumis à une évaluation intéressée. Une habitude conceptuelle et lexicale oppose les termes de *surveillance* et de *liberté*, dont la massive frontalité empêche de saisir que la densité et la puissance de la matrice n'induisent pas d'abord une *privation de liberté* mais instaurent un *nouveau paradigme relationnel*.

Corps médiatisés par des systèmes électroniques évolutifs, destinés à les *cartographier* sur un diagramme global, autant qu'équipés de technologies aux applications multiformes, notamment celle de quantifier multicritères la *qualité* d'autrui, avant toute mise en contact physique hautement informée. Disparition d'une part irréductible dans la relation à l'autre au profit de sa *réduction* en surface *consultable*, située dans l'espace et dans l'*historique* de ses gestes. Contrairement à ce qui s'énonce avec trop d'évidence, la prolifération des dispositifs de suivi ne constitue pas un danger liberticide mais entraîne une modification de nature anthropologique du principe d'*altérité*, sous la forme d'une *mise à nu* des identités pouvant être pénétrées suivant différentes techniques et différents niveaux d'appréhension : déplacements, pouvoirs et désirs d'achat, états thérapeutiques, jusqu'à un nouveau type de psychologie robotisée. La vie de chacun se confond avec une masse de calculs traités et *accessibles* d'après des canaux hétérogènes et des puissances variées.

Sous le même vocable de « surveillance », demeuré historiquement identique, il faut saisir une transformation de la nature du phénomène, de ses

modalités et de ses objectifs, non plus appelés à produire des effets coercitifs mais à favoriser au contraire une liberté d'existence, capable au cas par cas de *renseigner* le plus pertinemment possible sur la valeur de chacun au sein d'une cartographie dynamique et globale. La surveillance du XXI^e siècle ne cherche pas à intimider et à limiter, elle chercherait plutôt à exalter la puissance libidinale de vie et à distribuer ses *traces* à l'intérieur de systèmes d'expertise spécifiés, mis en réseau et toujours plus interopérables. Configuration surdéterminée non par un vecteur exclusif ou prioritaire – technologies numériques, incertitudes géopolitiques, sophistication marketing – mais par un *entrelacs* épigénique et complexe de forces différenciées, dont il est possible d'extraire la seule dimension véritablement isolable, qui contribue à l'étendre et à l'intensifier sans fin, à la permanence probablement transhistorique, mais aux niveaux d'intensité variables au cours du temps : la sensation trop humaine de la *peur*.

Nous sommes entrés depuis septembre 2001 dans un nouvel « *âge de la peur* », pour reprendre les termes de Nietzsche. La peur qui conduit à se prémunir *à tout prix* de l'imminence de la catastrophe, à instaurer le paradigme sécuritaire comme une des priorités politiques et juridiques majeures, à évaluer *a priori* toute personne ou tout acte en regard de son degré supposé ou *calculé* de dangerosité, à infiltrer espaces et corps de systèmes de contrôle et d'alerte. La peur qui conduit progressivement à faire plier le droit au profit de logiques « précognitives » aptes à pénétrer les intentions et à opérer des effets intériorisés dans la conduite des actes quotidiens. La peur qui pousse à envisager la surface désormais « plate » du monde comme un champ de bataille *préventif* : « La dialectique du terrorisme et du contre-terrorisme à l'échelle mondiale, en commençant par l'attentat du 11 septembre et la “guerre au terrorisme” du président Bush, risque de s'inscrire dans la version catastrophique de ce que nous avons appelé [...] la “dialectique du bourgeois et du barbare”. [...] Si la modernité a été une immense entreprise d'embourgeoisement du barbare, elle peut aussi produire le mouvement inverse de “barbarisation du bourgeois”, en réaction au terrorisme¹. » La peur encore induite par l'*affrontement* ultraconcurrentiel contemporain qui interdit tout retard stratégique, toute relégation vite définitive et oblige à une *agressivité* apparemment indolore mais réelle à l'égard des consciences.

La *peur panique*, capable d'ébranler de profondes catégories historiques supposées à tort définitivement acquises : « C'est justement au moment où elle voudrait donner des leçons de démocratie à des cultures et à des traditions différentes, que la culture politique de l'Occident ne se rend pas compte qu'elle a totalement perdu les principes qui la fondent². » La peur qui édifie sournoisement un catalogue lexical appelé à imposer dans les faits l'exigence de transparence intégrale, à l'instar de l'assise dictatoriale assurée dans 1984 par la suprématie croissante de la « novlangue ». Quantité d'expressions aujourd'hui témoignent de l'impératif de la surveillance comme couche

préalable à tout fonctionnement *garanti* de la socialité ou de soi, suivant un registre polymorphe qui confirme son infiltration tous azimuts : « guerre contre la terreur » ; « principe de précaution » ; « appels publics à la vigilance » ; rapport au corps marqué par l'omnipotence du verbe « surveiller » : son poids, sa tension, son alimentation...

Il faut relire Victor Klemperer qui écrivait en 1947, dans *La Langue du Troisième Reich* : « Le nazisme s'insinua dans la chair et le sang du grand nombre à travers des expressions isolées, des tournures, des formes syntaxiques qui s'imposaient à des millions d'exemplaires et qui furent adoptées de façon mécanique et inconsciente³. » La fixation de l'instinct de peur conduit à évaluer *d'abord* les risques avant toute entreprise, formant peu à peu un environnement au sein duquel toute initiative se perçoit comme un germe en puissance d'une fin catastrophique et non pas l'occasion d'une ouverture heuristique. Judith Shklar, philosophe politique américaine, avait affirmé dès le début des années quatre-vingt-dix que « l'avenir de nos sociétés est d'être des démocraties de la peur⁴ », tétanisées par une inhibition qui entraîne avec elle une infinité de conséquences plus ou moins manifestes, d'ordre politique, économique, culturel, toutes imprimées par la volonté craintive de *quantification préalable*.

« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes » (Déclaration universelle des droits de l'homme, 1948, article 12). « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques » (loi Informatique et Libertés, 1978, article 1^{er}). Déclarations dont on éprouve ici à quel point elles appartiennent à des périodes historiques somme toute récentes mais bien révolues. On peut affirmer sans risque que l'efficacité et la densité des protocoles de surveillance ne feront que s'accroître, que rien ne viendra *massivement* contredire leur expansion et leur sophistication continues. Une sorte d'étrangeté surgit dans le constat d'une indifférence tendancielle à l'égard de leur puissance et de leur expansion, entremêlant à la fois ignorance, naïveté et incrédulité.

« Toute l'humanité est éternellement schizophrène », disait Aby Warburg ; l'*ambivalence* des fonctionnalités offertes par les technologies miniaturisées (autant positives qu'objets de suivis individualisés) contribue encore pour une bonne part à ce phénomène surprenant d'insouciance collective, qui doit être rapproché dans sa collusion de confort et de *complicité* enchevêtrés aux paroles de La Boétie stigmatisant la propension humaine à se complaire dans un assujettissement pourtant théoriquement inacceptable : « C'est le peuple qui s'asservit et qui se coupe la gorge ; qui, pouvant choisir d'être soumis ou

d'être libre, repousse la liberté et prend le joug ; qui consent à son mal, ou plutôt qui le recherche⁵. » Indolence doublement entretenue par l'illusion à l'œuvre dans les sociétés démocratiques, qui suppose l'autonomie individuelle comme un principe fondateur absolument inébranlable, et par la relation aux objets devenus des *sujets* familiers et *parlants* de l'existence, certes souvent « indiscrets », mais finalement indispensables à toute vie bien *intégrée*, et s'inscrivant dans la quotidienneté avec une évidence naturelle et entendue : « L'habitude qui exerce en toutes choses un si grand pouvoir sur nous, a surtout celui de nous apprendre à servir et, comme on le raconte de Mithridate, qui finit par s'habituer au poison, celui de nous apprendre à avaler le venin de la servitude sans le trouver amer⁶. »

Nous avons à coup sûr atteint un « point de non-retour », dont la dimension irréversible n'est probablement pas perçue dans son inflexible réalité, et qui appellerait au préalable à toute réflexion et agissements positifs, une *lucidité* politiquement et socialement partagée : « C'est peut-être dans dix ou quinze ans qu'on pourra dire : finalement, tout a changé, notre sphère de liberté s'est réduite, mais on n'en était pas vraiment conscient. C'est un peu comme quand on est au bord d'un lac en train de s'assécher. Au début, vous ne vous en rendez pas compte, et un jour le lac est presque sec. C'est un phénomène qui peut être lent, progressif, pas forcément visible, mais incontestable. C'est pourquoi j'opère une analogie avec le réchauffement de la planète⁷. » Il faut se détourner à jamais de la chimère simpliste qui prétend *s'opposer* à des maillages qui se forment par accélérations exponentielles, s'intensifient d'après des proliférations multiformes de nature organique, hétéroclite, multicausal, qui nous dépossèdent en partie de nos pouvoirs historiques autrefois constitués à l'intérieur d'ensembles relativement stables, et nous obligent à repenser du tout au tout, au sein de ce complexe en fusion, la nature de nos véritables capacités, inaptes à empêcher une fois pour toutes l'essor de la matrice globale, mais qualifiées à *l'infléchir* indéfiniment.

À l'écart de toute perception massive des phénomènes et de l'illusion d'imaginer des solutions achevées, le foisonnement *inquantifiable* de faits et de paroles structurant les *dispositifs*⁸ de surveillance appelle l'élaboration sans relâche de *limites légales* aptes à indiquer les bornes, dont il est encore possible de *décider* qu'elles soient – au nom de principes démocratiques *inaliénables* – *absolument incontournables*. Kant insistait sur la nécessité d'encadrer les organes de pouvoir dans la mesure où « chaque personne abusera toujours de sa liberté si elle n'a personne au-dessus d'elle, qui exerce un pouvoir d'après les lois⁹ ». Dispositions qui dépendent des citoyens et du législateur, à qui il revient communément de s'emparer bien davantage de champs qui déterminent si *profondément* et *fermement* l'ensemble de nos sociétés. Il revient encore à chacun de nous, individus dotés de raison autant qu'utilisateurs de technologies certes efficaces mais *en tout point sensibles*, à *moduler* nos *usages*, à sortir d'une période ébahie et enivrée par la nouveauté

miraculeuse, pour entrer dans un autre moment probablement plus mature – une sorte de « seconde hypermodernité », non pas moins enthousiaste mais *éveillée* à l'égard de l'*animisme* inédit qui désormais rythme notre environnement pour le meilleur et pour le pire, qui appelle l'*ajustement* continu de nos pratiques, dans le risque et la *joie* de *ce qui vient* à la fois malgré nous autant que par le fait de nos puissances d'*adaptation* et d'*inventivité*, collectives et individuelles.

1- Pierre Hassner, « La revanche des passions », revue *Commentaire*, n° 110, été 2005.

2- Giorgio Agamben, *État d'exception*, *Homo Sacer*, op. cit., p. 35.

3- Victor Klemperer, *LTI, la langue du Troisième Reich. Carnets d'un philologue*, Paris, Albin Michel, « Bibliothèque Idées », 1996, p. 27.

4- Judith Shklar, *The Liberalism of Fear*, University of Chicago Press, publication posthume 1998, p. 27.

5- La Boétie, *Discours de la servitude volontaire* (vers 1548), Paris, Mille et une nuits, p. 12.

6- *Ibid.*, p. 21.

7- Alex Türk, « La majorité des Français n'ont pas conscience qu'aujourd'hui leur sphère de vie privée est en cause », *chat* modéré par Jean-Marc Manach, www.lemonde.fr, 10 juillet 2007.

8- Notion ici exactement entendue dans une perspective foucauldienne : qui inspire des écrits, des règlements, des conduites, des agencements spatiaux... « Ce que j'essaie de repérer sous ce nom c'est [...] un ensemble résolument hétérogène comportant des discours, des institutions, des aménagements architecturaux, des décisions réglementaires, des lois, des mesures administratives, des énoncés scientifiques, des propositions philosophiques, morales, philanthropiques ; bref, du dit aussi bien que du non-dit, voilà les éléments du dispositif » (Michel Foucault, *Dits et écrits*, Paris, Gallimard, vol. III, p. 299).

9- Emmanuel Kant, *Idée d'une histoire universelle au point de vue cosmopolitique*, sixième proposition, 1784.



Flammarion